AFRL-RH-AZ-TR-2010-0027

Cyber Operations Virtual Environment

Jennifer L. Winner

Lisa S. Holt

Jasmine Duran

Eric Watz

Lumir Research Institute

195 Bluff Ave

Grayslake, IL 60030

SEPTEMBER 2010
Final Report

Approved for public release; distribution unlimited (Approval given by 88 ABW/PA, 88ABW-2010-6042, 15 Nov 2010).

AIR FORCE RESEARCH LABORATORY
711TH HUMAN PERFORMANCE WING,
HUMAN EFFECTIVENESS DIRECTORATE,
MESA, AZ 85212
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICES

AFRL-RH-AZ-TR-2010-0027 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

JOSEPH WEEKS
Program Manager

HERBERT H. BELL
Technical Advisor

JOEL D. BOSWELL, Lt Col, USAF
Chief, Warfighter Readiness Research Division
Air Force Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
30-09-2010	Final Report	From 09-2008 To 09-2010

4. TITLE AND SUBTITLE
Cyber Operations Virtual Environment

5a. CONTRACT NUMBER
FA8650-05-D-6502

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
63227F

6. AUTHOR(S)
Jennifer L. Winner
Lisa S. Holt
Jasmine Duran
Eric Watz

5d. PROJECT NUMBER
4924

5e. TASK NUMBER
AS

5f. WORK UNIT NUMBER
10

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Lumir Research Institute
195 Bluff Avenue
Grayslake, IL 60030

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
711 Human Performance Wing
Human Effectiveness Directorate
Warfighter Readiness Research Division
6030 South Kent Street
Mesa, AZ 85212-6061

10. SPONSOR/MONITOR'S ACRONYM(S)
711 HPW/RHA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-RH-AZ-TR-2010 - 0027

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited (Approval given by 88 ABW/PA, 88ABW-2010-6042, 15 Nov 2010).

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This report details an instructional Science and Technology (S & T) plan to address the United States Air Force's (USAF's) need to defend against and respond to cyber threats to their networks. The approach documented within this plan focuses on the joint optimization of human performance and technologies, with a focus on instructional theory and design and human factor considerations and methodologies. Recommendations put forth in this report are informed by a review of considerations for the design of instruction and implementation within a virtual environment. Successful implementation of this S & T plan should impact USAF instructional capabilities and training, ultimately benefitting the operational community by producing Airmen who are aware of the likelihood and attributes of cyber attacks, who can use various tools to detect the presence of and effects of cyber attacks, and who are prepared to fight through these attacks. Airmen who are prepared will have developed robust operational methods to continue during and after cyber attacks, and be able to use indicators of network/data-source/communications health to identify and ward off cyber attack.

15. SUBJECT TERMS
Cyber, contested environment, mission assurance, mission essential functions, advanced instructional systems, instructional design, virtual learning environment, learning objectives, scenario development, fidelity, performance assessment, performance feedback, human factors, sociotechnical systems theory, after-action review, training, Air & Space Operations Center, Intelligence Surveillance and Reconnaissance, Air Mobility, enterprise-level computer and network security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Harry K. Pedersen
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED	73	**19b. TELEPHONE NUMBER** *(include area code)* 480-988-6561 x414

This page intentionally left blank.

Contents

List of Figures

Acknowledgement/Disclaimer

This work was sponsored by the Air Force Research Laboratory, under grant/contract number FA8650-05-D-6502. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Research Laboratory, the Department of Defense, or the U.S. Government.

The authors would like to acknowledge the efforts of numerous team members and contributors, as listed in Appendix A.

1 Forward

This report details an instructional Science and Technology (S & T) plan to address the United States Air Force's (USAF's) need to defend against and respond to cyber threats to their networks. The primary contract objective (CONTRACT NO.: FA8650-05-D-6502) was to formulate an S & T plan to exploit instructional science to shape modeling and simulation technology for training to prepare Airmen to fight through contested cyberspace thereby assuring mission success for mission-critical tasks and functions.

The effort involved reviews of current literature pertaining to sociotechnical systems theory, instructional theory and design, trust in automation, visualization, signal detection theory, and performance assessment. It also included outreach to operational and threat experts, scientists, and engineers working in relevant areas. Included in this effort was a survey of the current state-of-the-art tools and systems in the domain of cyber simulation and training. This effort is the result of coordination with a large number of individuals whose affiliations include Air Force Research Laboratory Information Directorate, Human Effectiveness Directorate, 505th Command and Control Wing, the Air Force Air Warfare Center, 57th Information Aggressor Squadron, 547th Intelligence Squadron, the 688th Network Warfare Wing, the 39th Information Operations Squadron, the 67th Network Warfare Wing (see Appendix A for a list of team members and contributors).

This instructional S & T plan is organized as follows. Section 2 discusses the need to defend in cyberspace and the increasing frequency of cyber threats, summarizes sociotechnical systems theory, overviews relevant human factors topics, and concludes with an overview of the S & T plan. Section 3 discusses considerations for the design of instruction, including instructional design, learning objectives, instructional theories, scenario development, evaluation, and performance measurement. Section 4 discusses considerations for the implementation of instruction in a virtual environment. This involves central components that replicate the operational environment, and supporting technologies which enable the instructional supports necessary for a virtual *learning* environment (VLE). This section concludes with a discussion of relevant design concepts that might inform the design and development of a virtual learning environment. Finally, Section 5 discusses the instructional recommendations resulting from this effort. The recommendations include general instructional recommendations and a discussion of modifications required for the development of a cyber practice and learning environment for the Air & Space Operations Center (AOC).

2 Introduction

The Department of Defense (DoD) relies heavily on information technology and network-enabled capabilities to achieve their objectives. The USAF's reliance on the Global Information Grid (GIG), enabling widespread information sharing, reflects the acceptance of the tenants of network centric warfare (NCW) theory. The theory proposes that (1) a networked force will improve information sharing; (2) information sharing will facilitate shared situation awareness (SA); (3) shared SA will enhance collaboration and self-synchronization; and (4) self-synchronization will increase mission effectiveness (Alberts & Hayes, 2003).

> NCW is essentially about information. The power of NCW depends on the collection, processing, and dissemination of actionable information. It relies on an extremely complex network of interoperable subnets and systems, working as they are expected to in order to meet its potential. Large networks are theoretically fairly robust; however, nodes that are both unique

> and critical can be highly lucrative targets. In the case of NCW, a potential adversary might attempt to work against any or all of the three NCW grids (sensor, information, and engagement), the connectivity that binds them together, or the information technology that underpins them all (Kamradt & MacDonald, 1998, p. 24).

Reliance on networked information systems, although it provides certain advantages, does not come without potential vulnerabilities. An early report by Buchan (1999) warned that hostile forces may attempt to affect USAF information systems. Recent events support the assertion that hostile forces are motivated to degrade capabilities, disrupt the coordination and decision making enabled by networked systems and/or exploit the network resources for their advantage (e.g., Meserve, 2009; Shane & Drew, 2009). The USAF has initiated numerous efforts in response to such threats, including the development of doctrine specific to cyberspace operations (United States, 2008).

2.1 Defining the Cyber Domain

The definition of the cyber domain is currently receiving a great deal of attention and may continue to change as work in this area matures (e.g., Mesic, Hura, Libicki, Packard, & Scott, 2010). For the purpose of this report we cite the following definition of cyberspace: "a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" (United States, 2008, p. 1).

It is important to note distinctions between cyber capabilities and cyber effects. Capabilities such as electronic warfare (EW) and psychological operations may create effects within the cyber domain (e.g., interruption of services) but they do not qualify as cyber capabilities (Vice Chairman of the Joint Chiefs of Staff, 2008). Examples of cyber capabilities include "computers, software tools, networks, cyber forces" (p. 1). "'Cyberspace operations' should encompass current computer network operations and activities to operate and defend the Global Information Grid" (p. 1).

The USAF recognizes the cyberspace domain as comprised of "many different network types with many different functions, levels of interconnectivity, technical complexity, and vulnerabilities" (United States, 2008, p. 6). The USAF also acknowledges the many challenges associated with reliance on other entities' networks such as civilian owned and operated infrastructure (Air Force Space Command, 2009). Terrestrial, airborne, and space nodes are critical to the USAF.

The complexity of the cyberspace domain and the DoD's reliance on civilian networks are not the only noteworthy concerns. Cases reported in public sources document that dangerous and more frequent cyber attacks on U.S. networks are occurring. For example, unknown software was discovered in the supervisory control and data acquisition (SCADA) system of a portion of the U.S. electric power grid (Merserve, 2009). In a news article discussing the increased cyber threat presence, Levine (2009) quoted Brig. Gen. John Davis of the U.S. Strategic Command who stated, "We are finding ourselves in an ever-increasing, sophisticated environment where our networks at [the Department of Defense] are increasingly in a contested environment". Davis also indicated that the U.S. military's technology teams deal with a wide variety of incidents every day. Further, nation states have demonstrated a willingness to use or to tolerate cyber attacks on sovereign nations. For example, Russia, to its own benefit, recently either perpetrated or tolerated denial of service (DOS) attacks on Estonia and Georgia (O'Connor, 2009).

Documentation regarding the current cyber threat landscape leaves little doubt that this domain is an area deserving of attention. The USAF's reliance on networked information systems requires that cyber threats be addressed to ensure that the benefits of NCW are maintained. According to Jabbour (2009),

"Cyberspace is viewed first and foremost as a foundational domain that enables US military superiority, and secondarily as another domain where the US can deliver effects" (pg. 11). The following section will summarize recent reports speaking to the USAF's current readiness level relative to threats in this domain.

2.2 Mission Assurance

Adversaries attack U.S. government and military computer systems daily. In a 2008 study (2008, page v), the United States Air Force Scientific Advisory Board (USAFSAB) stated, "Most observed activity is categorized as an 'information and network challenge' with limited observed impact on mission activities." However, the USAFSAB study members went on to conclude that during times of conflict it is likely that adversaries will shift their focus to disrupting mission operations, and that this level of warfare will include "zero-day exploits", i.e., attacks launched during the initial and following days of conflict.

According to the USAFSAB, Level I cyber warfare includes "attacks in which we observe system administrators 'warring' with hackers, mischief makers, and miscreants whose objective is to shut down systems and networks" (USAFSAB, 2007, Vol. 1, p. 16). They describe Level II cyber warfare as "attacks in which a cyber attacker might deliver a package which makes a [Surface-to-Air Missile] SAM think it is a Maytag washer" (p. 16). They went on to state that "Level III attacks are the ones to be feared; they are covert, they are planned, they are orchestrated, and they can cause widespread havoc and disruption without the victims realizing their problems are cyber-related. So, if an attack is 'commonly observed,' it is most likely not Level III" (p. 16). Attacks categorized within this level of warfare has been generically referred to by the USAFSAB (2007) as "malicious manipulation." The Final Report (Vol. 2) adds that the adversary will implement such manipulations within network mission applications, resulting in the allocation of mission resources to atypical activities with negative or non-optimal outcomes (USAFSAB, 2007, Vol. 2).

According to the USAFSAB, a major area in need of focus is mission assurance, which they describe as "measures required to accomplish essential objectives of missions in a contested cyber environment" (USAFSAB, 2008, p. vi). According to the USAFSAB's findings, information assurance has garnered substantially more attention than has mission assurance. Along the same lines, they concluded that Airmen do not understand the full range of possible mission effects resulting from cyber attacks and that today's technology does not meet the needs relative to mission assurance.

To achieve the goal of mission assurance, it is essential to fight through such malicious manipulations, but this is complicated by the fact that these attacks may or may not involve insertion of malicious code. Infiltration might lead to database manipulation and produce circumstances where the use of compromised databases would have severe and negative consequences for operations. In sum, the intent of Level III cyber warfare is to degrade a commander's situational awareness (SA), and to undermine confidence in decision-making and command and control (C2) processes that foster realization of a commander's intent. Paraphrasing the USAFSAB, the distortion of a commander's SA via cyber manipulations can cause friendly forces to miss a fight altogether, at best leading to disruption of actions and at worst leading to defeat.

Figure 1 (adapted from the 2008 USAFSAB study *Defending and Operating in a Contested Cyber Environment)* depicts how the intensity and level of cyber warfare is expected to change as the nation shifts from periods of day-to-day operations through crises into armed conflict. The figure illustrates an expectation that that the intensity of cyber warfare will increase and the level of warfare will be elevated to include malicious manipulations (Level III-type attacks on mission capability).

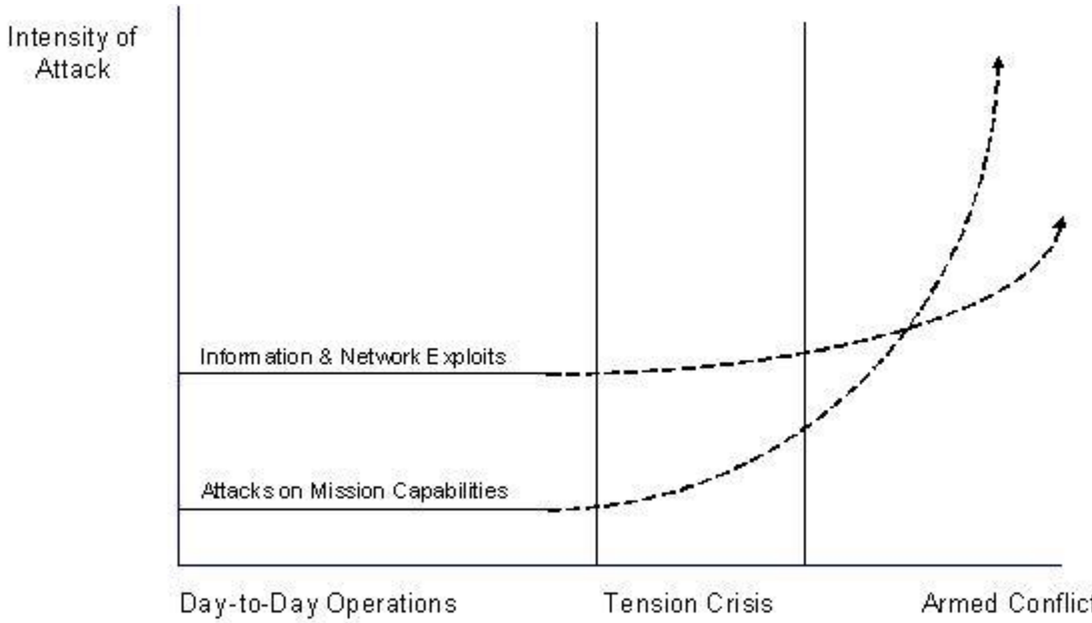

Figure 1. Expected change in levels of cyber warfare from day-to-day operations to armed conflict

It is likely that malicious manipulations introduced by trusted insiders – persons who have passed all of the peripheral security checks (background, physical, electronic), who have direct, trusted access to operational systems and networks, and who are acting against the interests of the country – will have the most devastating effects on a mission. Trusted insiders are in a position to alter databases, attack communications links, software or hardware, and all of this occurs with low risk of detection and attribution. Further, it is essential to maintain a current understanding of the Level III cyber warfare that will: (1) have a high negative impact on a commander's confidence in the C2 and decision-making infrastructure, (2) be very difficult to detect, and (3) easily infiltrate the network. It is also critical to understand that the types of attacks initiated by trusted insiders may also be introduced by electronic infiltration as opposed to physical breaches of security measures or direct physical contact with a system. Developing an understanding of such threats is essential for the preparation of vigilant Airmen who are able to fight through attacks and achieve success in their missions.

Among the USAFSAB's recommendations is a focus on enhancing mission assurance for mission essential functions (2008). Such functions include the C2 operations conducted in AOC (Weeks, 2009), air mobility operations (Levis, 2009), and Intelligence, Surveillance, and Reconnaissance (ISR) operations (Zacharias, 2009). The USAFSAB noted lack of existing tactics, techniques and procedures (TTPs) for 'fighting through' relative to these mission essential functions and a need for future efforts focused on the formulation of cyber defense TTPs (USAFSAB, 2008).

We judge both cyber operations, described as "current computer network operations and activities to operate and defend the Global Information Grid" (Vice Chairman of the Joint Chiefs of Staff, 2008, p. 1), and the mission assurance focus described by the USAFSAB to be important focus areas for the USAF. These unique areas imply a focus on different users. Cyberspace operations and defense of the GIG implies a focus on the enterprise-level network administrators and network security experts, whereas mission assurance for mission critical functions such as the AOC implies a focus on operators. *Focus solely on one group alone is not sufficient to achieve the USAF's operational goals and objectives*. The

complementary knowledge, skills, and tasks of these different users are essential for an integrated response to cyber warfare.

2.3 Sociotechnical Systems Theory

In response to the threats and complexities of cyber warfare, we have adopted sociotechnical systems theory as the basis for this S & T plan. Sociotechnical systems theory maintains that “organizational objectives are not best met by the optimization of the technical system and the adaptation of a social system to it, but by the joint optimization of the technical and social aspects” (Cherns, 1976, p. 784). Pasmore (1988) provided the following detailed characterization of this approach:

> The sociotechnical systems perspective considers every organization to be made up of people (the social system) using tools, techniques and knowledge (the technical system) to produce goods or services valued by customers (who are part of the organization’s external environment). How well the social and technical systems are designed *with respect to one another and with respect to the demands of the external environment* determines to a large extent how effective the organization will be. (p. 1)

Pasmore (1988) also characterizes an organization’s environment as extremely complex and continuously changing. Such may be said of the environment in which the USAF is currently operating, especially given the emergence of cyber threats. Already, the USAF has implemented changes in the social and technical systems in response to these environmental changes. Core cyberspace operations have been organized under the AFSPC major command, 24th Air Force (AF) subordinate element. The cyber force has been reorganized and changes have been made in enlisted and officer job specialties. Fifteen previous enlisted communications specialties have been reorganized under a cyber support specialty with several sub specialties. Also, a new enlisted specialty was created. The 33S officer communications specialty has been redefined as Cyber Operator and a new officer specialty has been created. Initial-skills and advance training in Air Education and Training Command (AETC) have been changed to support this restructuring of job specialties. Definition of knowledge, skills, and experiences required by a variety of Air Force Specialty Codes (AFSC) has also been a focus of recent work (e.g., Aptima, Inc., 2008, 2009, 2010). Finally, the development of the Combat Information Transport System (CITS) represents a change to the technical system (Air Force Communications Agency, 2007a, 2007b).

These examples illustrate that the USAF is currently modifying both its social and technical elements in response to perceived environmental changes. According to sociotechnical systems theory, neither type of effort alone will be successful in adequately addressing the effects of cyber attacks as both system elements are tightly coupled in operational settings. Rather, efforts guided by sociotechnical systems theory, which acknowledges that changes one makes to either system element (social or technical) will affect the other, is best suited in this instance.

A focus on both AF technology and people is in line with recommendations made by the USAFSAB (2007b).

> It is tempting to think of cyber warfare as primarily a technological conflict; however, for almost all operations that use computers, people are an integral part of the process. Thus, the security of an operation and the resistance to cyber attack depends not only on the inherent technical sophistication of the computer systems, but also on the knowledge and awareness about security issues of people using the systems. (p. 36 – 37)

“Sociotechnical theory is as concerned for the experience of humans within systems as it is with the system’s ultimate performance” (p. 487, Walker, Stanton, Salmon, & Jenkins, 2008). Based on the complex nature of the cyber domain and the dynamic nature of the environment in which USAF Airmen

are operating, the most effective approach is joint optimization of technology and Airman performance with the goal of creating "cohesive, expert, flexible teams that relate well to a wider system" (Walker et al., 2008, p. 495). Effective cyber defense efforts should leverage distributed expertise and rely on integrated teamwork for a unified response. The capabilities, limitations, and needs of individuals, teams, and teams of teams demand consideration alongside the technologies they utilize to complete their missions during cyber exploitation, malicious manipulation, and attack against ground, air, and space networks.

2.4 Human Factors

The methods and techniques from the field of human factors are congruent with sociotechnical theory (Carayon, 2006). Human factors is concerned with the interaction between humans and the tools they utilize to complete their work. This field aims to best match the work tools and processes to the humans based on their needs, capabilities, and limitations (Sanders & McCormick, 1993). Human factors practitioners aim to maximize the effectiveness and efficiency of the human's work and improve the experience of humans through the use of system design, environmental design, training, process design and personnel selection (Proctor & Van Zandt, 1994). The application of methods and processes from the field of human factors has shown to be successful within the military domain. The Tactical Decision Making Under Stress (TADMUS) Program provides an example of such success (see Cannon-Bowers & Salas, 1998; Collyer & Malecki, 1998).

The optimization of human and technological elements in response to cyber threats will require consideration of possible system failures. The USAFSAB (2008) characterized the relevant tasks for Airmen to successfully fight through to include detect, assess/attribute, protect, respond, and recover/reconstitute from system faults resulting from cyber attacks. Topic areas discussed within the human factors literature have focused on the identification of skills, processes, and training to enable individuals to deal effectively with automation system failures. These topics are relevant to the needs of Airmen operating in the current cyber threat environment. Accordingly, the following sections summarize some relevant topics from the field of human factors.

2.4.1 Fault detection

The field of human factors engineering has provided a documented history of the study of detection tasks. Work in this area has resulted in methodologies for evaluating the effectiveness of various detection tools and methodologies. Performance in target detection or decision-making tasks is often assessed by examining percentages of correct decisions. However, interpretation of these correct detections is not straightforward as there are two possible ways to arrive at a correct detection. In the first case, the individual is actually skilled at target identification, applying knowledge to correctly identify the target. In the second case, the correct identification is accidental, possibly because the person defaults to identifying most cases as a target. Signal detection theory (Swets, Tanner, & Birdcall, 1961) defines a model of perceptual processing that provides an estimate of detection capability independent of the operator's willingness to make target responses (See, Macmillan & Creelman, 1991; Parasuraman, Masalonis, & Hancock, 2000).

The application of signal detection theories will be useful in determining whether an instructional program, manual process, or automated tool increases the proportion of correctly detected cyber attack signatures and/or minimizes the proportion of missed attack signatures. Additionally, signal detection theories may facilitate assessment of detection rates for cyber attack signatures among the noise of routine system malfunctions. Signal detection theories may have direct explanatory power in cyber attack detection instruction.

2.4.2 Fault diagnosis

Fault diagnosis is another topic area from the human factors literature which can inform the preparation of Airmen to effectively counter cyber attacks. A major focus of such efforts has been on fault diagnosis training (Duncan, 1987; see also Reason, 1990). Prior work has focused on the determination of heuristics commonly employed by those experienced in fault diagnosis (e.g., Duncan, 1987) as well as the design and evaluation of diagnostic strategies (e.g., Ham & Yoon, 2007; Dammon & Lane, 1993).

The USAFSAB's anticipation of increased cyber attack intensity and the inclusion of "zero-day exploits" (2007a) leads us to conclude that diagnosis of multiple simultaneous system faults (Patrick et al., 1999; Reising, 1993) and novel faults (Duncan, 1987; Yoon & Hammer, 1988) are relevant in a cyber warfare context. Troubleshooting skills relevant to technological system failures have been identified within the literature (Morris & Rouse, 1985) and training protocols for structured troubleshooting have been shown to be effective in some cases (e.g., Schaafstal, Schraagen, & van Berlo, 2000). However, it is important to note that limitations do exist. As discussed by Duncan (1987) and Reason (1990), anticipation of possible but never before seen system faults is difficult. Although fault diagnosis training may be effective to some extent, it will not guarantee successful diagnosis, especially when dealing with novel faults (Duncan, 1987).

2.4.3 Trust in networked systems

The threat of cyber warfare has renewed interest in another human factors topic—trust (e.g., Miller, 2009; USAFSAB, 2007a, 2007b, 2008). According to the USAFSAB, operational systems may be "operational but degraded" (2007a, p. 22). Successful cyber attacks are expected to affect the reliability of networked system and therefore are expected to affect the trust that individuals place in those systems. It is widely maintained that one's trust in an automated system affects reliance on that system (e.g., Dzindolet, Peterson, Pomranky, Pierce, & Beck, 2003; Lee & Moray, 1994; Lee & See, 2004; Merritt & Ilgen, 2008; Parasuraman & Riley, 1997). Empirical findings indicate that system failures negatively impact trust, reliance, and task performance (Rovira, McGarry, & Parasuraman, 2007).

Performance decrements attributable to decision aid failures may be mitigated through the use of meta-information regarding aid performance (Seong & Bisantz, 2008). Explicit feedback regarding system errors and system reliability has been found to affect both trust (Dzindolet et al., 2003; de Vries, Midden, & Bouwhuis, 2003) and reliance (McGuirl & Sarter, 2006). Training has been shown to be effective for calibrating trust. For example, Masalonis (2003) demonstrated that cueing individuals to situations in which automation reliability will vary is effective for achieving appropriate trust calibration. Future work will likely assess the applicability of the findings from this literature in operationally relevant contexts and in instances of networked information system failures resulting from malicious intent.

2.4.4 Human factors: Summary

These human factors topics represent a small sample of those with potential to inform future efforts in the cyber domain. These topics are relevant to the joint optimization of human performance and technology and were selected because of their relevance to system failures. Airmen who are equipped with intrusion detection systems (IDS) are able to fuse information from multiple sources to conduct analysis of the threat landscape. Alternatively, in some cases, Airmen are not equipped with IDSs, nor are they trained on the indicators of attacks. Any such gaps in technology and/or skills are troubling given the USAFSAB's characterization of the functions required for mission assurance.

Fortunately, recent efforts relevant to these areas have shown promising results. A series of efforts have been conducted to evaluate instructional materials designed to help individuals avoid phishing

attacks (Kumaraguru & Sheng, 2008; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010; Sheng, et al., 2007) and, more recently, spear phishing attacks. In one study, the data indicate a 40% reduction in the tendency to provide information to phishing websites (Sheng et al., 2010). We anticipate a substantial increase in efforts focused on technological and instructional considerations relevant to detection, assessment, response, and recovery from attacks in the cyber domain.

2.5 Overview of S & T Plan

As an S & T effort of Air Force Research Laboratory (AFRL), this plan is not intended to directly support operations or the development of operational tools. Rather, successful implementation of this S & T plan should impact USAF instructional capabilities and training, ultimately benefitting the operational community by producing Airmen who are aware of the likelihood and attributes of cyber attacks, who can use various tools to detect the presence of and effects of cyber attacks, and who are prepared to fight through these attacks to achieve mission assurance. Airmen who are prepared will have developed robust operational methods to continue to fight during and after cyber attacks, and be able to use indicators of network/data-source/communications health to identify and ward off cyber attack.

2.5.1 Focus on instruction

The motivations to focus on instructional capabilities are many. Richard White (67th Network Warfare Wing [NWW]) described a need for instruction to enable interactive, realistic training (Hershey, 2008):

> Network Warfare and Operations Distributed Training: The AF requires the ability to perform on-line and distributed network warfare and network operations training across the AF's networks. In order to provide a more effective and realistic training environment, the AF requires the implementation of a distributed network training environment. This will allow multiple units conducting network warfare (NETD [Network Defense], NETA [Network Attack], NET C2) and network maintenance and sustainment operations (INOSC [Integrated Network Operations and Security Center], APCs [Area Processing Center], ESUs [Enterprise Service Unit], NCCs [Network Control Center], etc.) to train together on-line. This distributed training implements the 'train as you fight' concept. Network operations are not done independently, requiring the synchronized and simultaneous actions by multiple operators (p. 1).

Another important motivation stems from the cyber work force development needs documented by United States Strategic Command (USSTRATCOM) (Trefz, 2008). Some of the needs noted include tools to reduce training time, instructional capabilities beyond traditional lectures, and tools for training at both the individual and group level.

Similarly, the findings of the USAFSAB studies (2007a, 2007b, 2008), which summarize operational, technical, and academic viewpoints, also suggest a focus on instruction. The USAFSAB findings were clear: USAF Airmen should be trained to recognize cyber threats, to develop and initiate effective counter-measures, and to fight through – that is to assure mission success in a non-permissive, contested, cyber environment. As discussed in Section 2.2, the behaviors of recognizing, responding to, and fighting through are important aspects of mission assurance. As US forces become more integrated and net-centric, mission assurance capabilities need to improve to minimize the probability that cyber attacks will significantly damage USAF war-fighting capability. The USAFSAB made numerous recommendations, including development of war games, training, exercises, and experiments in contested cyber environments. Further, some of the actions recommended by the USAFSAB place a heavy emphasis on instruction and training research – aimed at increasing the cyber situation awareness of all Airmen and women — not simply the cyber experts.

The National Academy of Engineering (NAE) (2008) acknowledges securing cyberspace as one of the 14 grand challenges for the field of engineering, pointing out that information networks are an integral part of nearly every aspect of modern life, including military capabilities. The NAE recognizes both the technical and human aspects that must be addressed to achieve a solution. Additionally, they have focused their attention on the enhancement of virtual reality because of its potential for training in a variety of domains. Personalized learning is also among the challenges acknowledged by the NAE. Such an approach to instruction is focused specifically on individual needs.

A final important motivation to be acknowledged is the prevalent use of virtual environments for training throughout the USAF. It is important to note, however, that merely providing opportunities for practice is not sufficient to ensure that learning will take place (e.g., Milham, Carroll, Stanney, & Becker, 2009). Accordingly, the S & T plan outlined in this document exploits instructional science, methods and approaches from the field of human factors engineering, and state-of-the art modeling and simulation technologies to simultaneously evolve human skills and technological capabilities for appropriate response to cyber attacks through the design of advanced instructional systems.

2.5.2 Scope of the instructional S & T plan

This instructional S & T plan outlines efforts with potential to impact Airmen in a variety of ways, including increasing awareness of safe computing practices, increasing awareness and detection of cyber threats and attacks, and enabling Airmen to fight through attacks to achieve mission assurance. This instructional S & T plan will address mission essential functions such as C2 operations (AOC), ISR operations, air mobility operations, and cyberspace operations (i.e., “defending the GIG”). These efforts will focus on promoting integrated teamwork by Airmen whose operational activities rely on a variety of networked systems.

Cyber-relevant S & T efforts must recognize Airmen as distributed sources of expertise with ready access to important information needed to guard against, recognize, and fight through cyber attacks. Given the reliance on technology, and the reciprocal relationship between instruction and technology, the development of virtual environments to support learning in the cyber domain will require careful implementation of instructional design processes, focusing on both the operational and learning challenges facing Airmen as they are confronted by cyber threats.

Achieving the objective of well-trained Airmen who are able to effectively fight through cyber attacks will not come simply. The technology, processes, training, and instructional systems are evolving concurrently. Due to the lack of cyber-relevant TTPs for some mission critical functions (as noted by the USAFSAB, 2008), S & T efforts are needed to inform TTP development. From a joint perspective, disparate systems and configurations utilized by the different military departments ensure that there is no one solution for mission assurance. Because the departments are responsible for and have authority to conduct their business differently, proposed processes, products, and training will not apply uniformly across the board, but will need to be adapted appropriately to address the needs of each department.

The following sections will detail the instructional focus and scope of this plan. Section 3 will discuss the essential steps in instructional design, with emphasis on the establishment of learning objectives and their importance throughout the design process. Section 4 will discuss important considerations for implementation of instruction in a virtual environment, including the required fidelity of the environment, the supplemental technologies needed to support learning, and research-based design concepts. Finally, Section 5 will describe a number of recommended efforts, each of which will contribute to the science of virtual learning environments, and help achieve the goal of producing

Airmen who have the knowledge and skills to detect, assess/attribute, protect, respond, and recover/reconstitute from cyber warfare (see USAFSAB, 2008).

3 Considerations for the Design of Instruction

In the design of advanced instructional systems to address threats in the cyber domain, one must adopt a learner-centered design (LCD) approach, focusing on the individuals as learners. Learners are essentially novices who will require support as they learn to perform new tasks. Instruction must be designed to assist the learners as they perform unfamiliar tasks and also help them learn the underlying knowledge and skills associated with the tasks. The learner has unique needs (Soloway, Guzdial, & Hay, 1994), requiring support to engage in the new processes, to make sense of the new content, and to articulate their developing understanding. Although the LCD process must address issues of usability, it must primarily focus on the conceptual gulf between the novice and the expert (Quintana, Krajcik, & Soloway, 2001, 2003). An analysis of the operational tasks and an understanding of the learner's current knowledge state/skill level will result in specification of learning objectives and the support that the learner will need to achieve the objectives. Good learner-centered systems provide needed guidance and support so that the learner can engage in the new, unfamiliar task while gaining expertise.

Instructional systems design (ISD) models lay out a process for designing instruction. The field of instructional design is rooted in cognitive and behaviorist theories of learning. ISD processes can maximize the effectiveness of an instructional system by determining the learning needs, establishing instructional objectives, and designing the instructional intervention to address the objectives. ISD processes also include an evaluation component that is tightly linked to the learning objectives. There are many ISD models, but most follow the form of the Analysis Design Development, Implementation Evaluation model (ADDIE) (Molenda, 2003), having the following steps:

1. **A**nalysis: Establish instructional goals and objectives. Identify important characteristics of the learner's existing knowledge and skills.
2. **D**esign: Select instructional strategies and create prototype.
3. **D**evelopment: Create the instructional content.
4. **I**mplementation: Subject learners to the instructional system.
5. **E**valuation: Evaluate the efficacy of the instructional system.

Milham et al., (2009) outline a process for the design of instructional systems that addresses the components of the ADDIE model.

- Analyze the operational context to understand the tasks. (Analysis)
- Define learning goals in terms of how tasks are performed in the operational environment. (Analysis)
- Decompose learning goals from a human knowledge standpoint into knowledge and skills required for successful performance (ultimately defining performance measurement metrics). (Analysis and Evaluation)
- Develop scenarios and manipulation variables to manage the training experience. (Design and Development)

Cohn, Schmorrow, Lyons, Templeman, and Muller (2003) outline a process that begins with the identification of learning objectives, but is heavily focused on evaluation. The six components of their design process are:

- Task analysis: Focusing on behavioral aspects of a task performed in an operational setting. Identifying learning objectives and scenario elements that will support them.
- Human computer interface evaluation: Identifying requirements for sensory modalities in the environment.
- System usability: Iteratively evaluating the usability of the environment.
- Virtual Environment (VE) user considerations: Evaluating side effects and after effects of the virtual environment.
- Team performance: Documenting how well the environment supports team performance.
- Training transfer: Documenting the degree to which skills transfer from the environment to the operational environment.

As most instructional design processes address the components of the ADDIE model, the following sections will summarize the research and literature that is relevant to each ADDIE component.

3.1 Analysis: Specification of Learning Objectives

The most important part of any ISD process is the analysis step, in which the objectives are defined. The objectives essentially specify what the learner should be able to do upon the completion of the instruction. These objectives lead directly to the development of performance measures which can be used to provide feedback during or after the instruction.

Learning objectives serve as the backbone of any instructional system. They are used to drive scenario development, instructional interventions and performance assessment. The success of the event-based approach to training (Fowlkes, Dwyer, Oser & Salas, 1998) stems from its capability to provide practice opportunities on targeted objectives. Without a good understanding of the operational requirements, the instructional system could lack vital information that is necessary for task execution.

Two distinct types of requirements analyses can be used to produce the objectives and the corresponding performance metrics (Milham et al., 2009). Operational requirements analysis (ORA) focuses on the identification of objectives that are both appropriate for the context of the domain and the expertise of the learners. ORA is concerned primarily with the constraints of the domain, i.e., the target operational environment and mission context). The output of ORA is then fed forward to human performance requirements analysis (HPRA), which essentially translates the learning objectives into performance metrics. HPRA integrates an understanding of human performance and learning to measure the achievement of the learning objectives. HPRA will be discussed in more detail in Section 3.4.2

3.1.1 Operational requirements analysis

Operational requirements are the building blocks of system requirements. They essentially specify the requirements to ensure that the system operates in a manner consistent with user needs and expectations (Fairley & Thayer, as cited in Milham et al., 2009). Central to ORA is a task analysis to identify the information processing requirements of the targeted tasks (e.g., the inputs the learner must receive and the outputs the learner must convey). As part of at task analysis, tasks are decomposed into subtasks, team member roles are specified, important tools are identified, and information flow is mapped out.

A fundamental outcome of ORA is a system whose fidelity requirements are based on learning objectives. They system replicates only the aspects of the operational environment which are essential

for the performance of tasks related to the instructional goals. This not only ensures an effective learning environment, but also a cost-effective one.

In military domains, learning goals can often be derived from information in training and readiness manuals. The manuals spell out the tasks that will be targeted (individual and team), and the desired level of performance. Military doctrine publications and Career Field Education and Training Plans (CFETPs) are other sources of information from which to derive learning goals. Documents such as the CFETPs identify the knowledge and skills and level of mastery required for each AFSC.

3.1.2 Competency-based training

In 2002, the DoD began an initiative to transform training based on the following vision (OUSD P&R, 2002):

> *Provide dynamic, capabilities-based training for the Department of Defense in support of national security requirements across the full spectrum of service, joint, interagency, intergovernmental and multinational operations.*

The key phrase in this vision statement is “capabilities-based” which implies a focus on mission performance and accountability, shifting the emphasis for training from platform operation to a higher-level capability, e.g., air superiority. Specification of learning objectives is essential for accomplishing this goal. The learning objectives must be derived from operational tasks, encompassing knowledge, skills, and abilities, and differentiations between exemplary and successful performers (Dubois & Rothwell, 2004). The objectives define a rich competency model against which performance can be assessed at many levels, provided corresponding performance metrics are developed to document obtainment of objectives.

The US Air Force has taken the DoD vision seriously and has implemented an important step towards true competency-based training. The Air Combat Command (ACC) defines competency-based training as “the ability to compare individual aircrew performance to a defined proficiency level, maintain acceptable levels of performance and target areas requiring improvement (Colegrove, 2004).”

The Mission Essential Competency (MEC) process (Alliger, Beard, Bennett, Colegrove, & Garrity, 2007; Colegrove & Alliger, 2002), which defines consistent performance measurement criteria across a single weapon system, creates a tight link between competency levels and learning objectives (Colegrove & Bennett, 2006). MECs are defined as “higher-order individual, team, and inter-team competencies that a fully prepared pilot, crew, flight, operator, or team requires for successful mission completion under adverse conditions and in a non-permissive environment” (Colegrove & Alliger, 2002). The MEC process has been described as a competency model that is determined through the use of job analytic techniques (Alliger, Beard, Bennett, Colegrove, & Garrity, 2007). The outcome of the MEC process has been utilized to develop simulation-based measures of performance (Schreiber, Watz, Bennett, & Portrey, 2003; Portrey, Keck, & Schreiber, 2006). MECs have also been utilized to identify training gaps and form the basis of assessments for determining the capabilities of a system for training (Prost, Schreiber, & Bennett, 2008; Prost, Schreiber, & Bennett, 2007; Prost, Schreiber, Bennett, & Kleinlein, 2008). It is important to note that the MEC process does not produce learning objectives per se, but rather has the potential to inform their development based on the definition of desired competencies. (A discussion of the existing cyber-related learning objectives for the AOC can be found in Appendix C. This discussion also includes an analysis of the AOC MECs.)

3.2 Design: Drawing from Instructional Theory

The design of instruction to address the learning objectives depends on a number of factors including nature of the domain, structure of the knowledge and skills to be learned, environment in which the knowledge must be applied and skills performed, etc. Instructional theories can inform decisions about difficulty of scenarios, form and timing of feedback, nature of hints and cues, the spacing of practice opportunities, and manipulations of the environment to enhance learning (Cannon-Bowers & Bowers, 2009). The following sections summarize a number of popular instructional theories and their implications for the design of instruction. Although some of the theories do not seem directly applicable to the cyber domain, each theory has important characteristics which can be implemented in some form.

3.2.1 Behaviorist learning theory

B. F. Skinner (1958) viewed learning as a "programming" process whereby a person's externally visible behavior could be shaped through a conditioning system of rewards and punishments. This behaviorist school of thought led to the development of a class of "teaching machines" often referred to as computer-based training (CBT) or computer-aided instruction (CAI). Immediate feedback is perhaps the most prominent feature of such learning environments. Learner's responses are compared to pre-programmed answers and appropriate positive or negative feedback is given. In addition, a pre-programmed rubric is used to determine whether the learner has successfully learned enough (i.e., gotten enough correct responses) to proceed to the next task. There is no mechanism to evaluate the learner's underlying knowledge or needs beyond this shallow level (Beck, Stern, & Haugsjaa, 1996).

The immediate feedback model employed in behaviorist learning has proven to be an effective instructional strategy in many domains (Anderson, Corbett, Koedinger & Pelletier, 1995; Anderson, Boyle, Farrell & Reiser, 1984). The behaviorist approach is most useful in cases where the tasks are narrowly defined and have clear answers. Because recognizing, responding to, and fighting through cyber threats certainly requires much higher-level thinking and problem-solving skills, the behaviorist theory is not particularly relevant, and the immediate feedback strategy may be challenging to implement.

3.2.2 Information processing or cognitive learning theory

In contrast to the behaviorist theory, which considers only observable behavior, the information processing or cognitive theory considers models of cognition which are based on the idea that "certain aspects of human cognition involve knowledge that is represented symbolically" (Anderson, 1983). Rules can then be applied to the representations to manipulate the knowledge, generate new knowledge, or make inferences. Human cognition can then be represented symbolically. Programs using these representations and rules can then be written as models that simulate human problem-solving behavior. The emerging field of cognitive informatics (Wang, 2007; Yao, 2004) addresses the underlying structure of knowledge and its impacts on information processing in both humans and computers.

An intelligent tutoring system (ITS) makes use of machine information processing in order to affect human information processing (i.e., learning). The defining feature of an ITS is that it carefully oversees a learner's work to provide needed guidance, i.e., individualized feedback is given. ITSs incorporate a rule-based expert model of the target skill which is used to monitor and guide novice learners as they engage in the new activity. The intent of an ITS is to model the actions and interventions of a human tutor which is the most effective means of instruction (Bloom, 1984). The ITS uses information about the task and the current state of the learner's knowledge of that task to make instructional interventions

(Corbett, Koedinger, & Hadley, 2001). The pedagogical nature of these instructional interventions is usually quite limited in nature. The model-tracing approach of many ITSs forces the learner to proceed in steps of a specified grain size (corresponding to the underlying rules) which constrains the progression of the learner's actions. If the learner makes a recognizable error (which has been pre-programmed as a buggy rule in the system, i.e., a rule reflecting the incorrect process leading to the error state), an error message is presented to explain why the action is in error. If the learner asks for help, a message is presented to guide the student toward the correct solution path. These error and help messages are not general, but instead are very context specific as they are generated based on a matching of the learner's solution with the underlying model of expert solution (Anderson et al., 1995).

The information processing or cognitive approach is useful in cases where the representation of the domain knowledge has a significant rule component. That is, the domain must not be primarily declarative knowledge with limited inferential reasoning (Anderson et al., 1995). This may seem constraining, but over the years there have been a wide variety of ITSs developed in a number of domains including geometry, medical diagnoses, mammography interpretation, physics problem solving, computer programming and algebra proofs. In the case of recognizing, responding to and fighting through cyber threats, the domain is probably not yet understood well enough to represent the desired knowledge as rules. However, the information processing or cognitive approach could be quite useful for representing the threat activity to which Airmen must respond. The model of providing guidance to the learner is also certainly applicable to in the cyber domain.

3.2.3 Social constructivist learning theory

The social constructivist theory encompasses important theories about how people learn. First, the social aspect of the theory asserts that "knowledge is… in part a product of the activity, context, and culture in which it is developed and used" (Brown, Colllins, & Duguid, 1989). This contextualized view of knowledge implies that learners must participate in social context that reflects the culture of the practice. Second, the constructivist aspect of the theory asserts that learners must be actively engaged to make cognitive connections between their existing knowledge and the knowledge they are learning (Papert, 1993; Piaget, 1954).

Because constructivism is a "theory of knowing" and not a "theory of teaching," there is no one specific constructivist approach (Bransford, Brown, & Cocking, 2000). As a result, the products of the social constructivist approach are complex learning environments rather than specific types of instructional systems. Learning environments can include multiple components that work together to support the learner as they mindfully engage in and learn a new practice. Wilson (1996) defines such a learning environment as: "a place where learners may work together and support each other as they use a variety of tools and information resources in their guided pursuit of learning goals and problem-solving activities."

Designers of learning environments are guided by a set of seven important pedagogical goals (Honebein, 1996). (1) Learners must be given some autonomy in the learning process so that they are actively engaged in the knowledge construction process. (2) Learners must experience multiple ways to think about and solve problems to enrich their understanding. (3) The learning must be situated in a realistic and relevant context to increase the likelihood of transfer from the learning context to actual practice. (4) The learner must be given some ownership in the knowledge construction process so that the role of the instructor becomes supportive rather than primary. (5) Collaboration must be encouraged so that the social interactions and roles of the practice can be realized. (6) Multiple modes of representation must be employed to demonstrate different perspectives and enrich the learner's knowledge. (7)

Metacognitive processes must be encouraged so that the learner can inspect and reflect upon his/her own thinking.

Depending on the context of the learning objectives, these goals may be instantiated in a variety of ways, leading to learning environments which look very different on the surface. A learning environment may be comprised of multiple components (e.g., teacher, curriculum, and ITS) which work together to support and guide the learner. Although it is possible to construct a learning environment that does not incorporate technology, it is more practical to include technology so that the driving goal of personally adaptive instruction can be more readily realized.

The social constructivist approach allows one to tackle more complex domains than either the behaviorist or information processing approaches, making it the most applicable learning theory for application in the cyber domain. Considering the potentially great gap between the novice learner and the desired performance, significant structure and support will be needed for the novice learner to effectively engage in the new practices.

3.2.4 Guidance, feedback, and scaffolding

Regardless of the instructional theory applied, learners are often presented with novel tasks that are beyond their abilities. Research has shown that learning can suffer when pure discovery or trial and error is the primary means of skill acquisition (Lane & Johnson, 2009). Pure practice without any instructional components is unlikely to be effective or efficient. Guidance is critical for success, as it increases the chances that learners will be successful. The intent is that with support they will learn to do them. This basic strategy is theoretically based upon Vygotsky's (1978) zone of proximal development (ZPD) concept. ZPD is defined as the zone of activity in which a person can produce with assistance what they cannot produce alone. Wood, Bruner, and Ross (1976) first introduced the idea of scaffolding as a process to take advantage of the ZPD. They define scaffolding as a process where assistance is provided to enable learners to successfully perform tasks that would be otherwise be too difficult. Pea (2004) points out that a fundamental aspect of the scaffolding process as an instructional strategy is fading. If the supports provided to the learner do not fade over time, the learner may become reliant on them and never achieve autonomous performance which is the goal in an instructional setting. Situations in which supports remain in place and continue to assist performance must be considered to be distributed intelligence (scaffolds-for-performance), not independent performance (scaffolds-with-fading) (Pea, 2004). Effective human tutors achieve a delicate balance of learner participation and guidance, allowing the learner to do as much of the work as possible, providing just enough feedback to minimize frustration (Lane & Johnson, 2009).

Although various researchers have proposed guidelines and strategies for implementing scaffolding, there exists no agreed-upon theory of pedagogical support nor mechanisms to describe successful scaffolding approaches (Quintana, et al., 2004). Guzdial (1994) first proposed three ways to scaffold and provide needed structure for difficult tasks: communicating process to learners, coaching learners with hints, and prompting for articulation and reflection. Pea (2004) recently proposed three additional scaffolding strategies: constraining tasks to reduce the degrees of freedom and increase chances for successful performance, focusing learner attention by highlighting relevant task features, and modeling advanced solutions. Although these guidelines for designing scaffolds are all theoretically grounded, there are no clear suggestions for how to implement them in the design of a learning environment.

In an attempt to guide actual design, Quintana et al. (2004) have proposed a scaffolding design framework that builds on current proposals of general scaffolding principles (Linn, Davis, & Eylon, 2004; CILT, 2004). This framework is theoretically grounded in: (a) cognitive apprenticeship (Collins, Brown, & Newman, 1989) which specifies how performance of complex tasks can be distributed with others

providing assistance, (b) cognitive models of learning by doing (Anderson, 1983; VanLehn, 1989) which specify expertise and learner difficulties, and (c) social constructivism (discussed previously). Quintana's (2004) framework organizes scaffolding guidelines around three central components of scientific inquiry: sensemaking, process management, and articulation and reflection. The guidelines spell out the kinds of support learners need to perform each of those inquiry activities. Explicit scaffolding strategies are then provided for each guideline which provides concrete ways these guidelines could be realized in design.

There are still no specific prescriptions for how to implement scaffolding. Specific design decisions must be based on context and an analysis of the learner's obstacles. The guidelines and strategies provided by research can guide these decisions. Scaffolding can be incorporated in any kind of instructional system. The strategies available for use however, are limited by the theory of learning which drives the instructional design, e.g., a richer array of scaffolding strategies are available for use in a constructivist learning environment than in an intelligent tutoring system.

3.2.5 Instruction in ill-defined domains

Instructional theories and instructional design models have typically been applied in well-defined domains (i.e., those in which there exists a systematic way to determine when a proposed solution is acceptable (Minsky, 1995)). Ill-defined domains on the other hand, lack such procedures and their tasks have the following key characteristics: They lack definitive solutions, the solutions are heavily dependent upon conception and formulation of the problem, and solutions require retrieval of relevant concepts and mapping them to the task at hand (Ashley, Chi, Pinkus, & Moore, 2004).

Recognizing and fighting through threats in a contested cyber environment certainly qualifies as an ill-defined domain, thus making it a challenge to develop instruction. The space of possible actions in the cyber domain is large and it may not always be possible to classify actions as correct or incorrect. Correct actions are highly dependent on contextual factors that vary greatly from situation to situation. The behaviors of actual cyber threats are constantly changing and not completely understood. Consequently, effective strategies to handle the threats are constantly evolving in response to the changing threats and are certainly not well formalized or documented.

How to train in ill-defined domains is a topic of interest in the intelligent tutoring research community. They have identified effective strategies employed by human tutors in ill-defined domains (Lynch, Ashley, Aleven, & Pinkwart, 2006):

- Studying cases (e.g., law, business, and architecture) can often highlight the constraints and nuances of the domain better than an abstract model. Case studies provide analogies on which to base work. Implementation of the case study strategy requires a great deal of interpretation which is done using Socratic dialogue between the student and instructor.
- Weak theory scaffolding provides a loose theoretical framework to structure the domain, and the restrictions of the theory are eventually faded out. This strategy makes the ill-defined domain more tractable.
- Expert review strategies elicit subjective judgments of and feedback performance rather than evaluating performance against formal theory.
- Peer review strategies draw on the unique perspectives of less expert peers, e.g., a brown-bag research talk or a critique of an artistic piece.

Current research in intelligent tutoring is focused on ways to implement these subjective strategies in computational learning environments, i.e., environments in which all guidance and feedback are provided by the computer rather than a human instructor.

3.3 Development and Implementation: Scenario Development

Once learning objectives have been established, they become the foundation for the development of training scenarios or exercises (Cannon-Bowers & Bowers, 2009). Various events or triggers can be embedded into the scenario to elicit particular behaviors related to the underlying learning objectives. Stringing a series of events or triggers together into a coherent scenario or story provides a realistic context and motivation for the targeted performance. Scenario-based training evolved from problem-based learning strategies which engage learners in authentic problems and scenarios in order to facilitate the transfer of skills to real-world contexts. Context-rich situations are used to trigger specific behaviors, thus addressing specific learning objectives (Shadrick & Lussier, 2009). The primary goal is to create scenarios that allow for practice of the learning objectives and enable measurement and diagnosis of performance (Milham et al., 2009). Scenarios can be developed to target different objectives over a range of difficulty levels.

Effective scenarios not only have to reflect the learning objectives revealed in the task analysis, but they must also remain current, taking advantage of lessons learned in operational settings. This requires a rapid knowledge elicitation processes to capture the expert knowledge of those in the operational environment. Shadrick and Lussier (2009) suggest the following methods for gathering that important operational knowledge:

- Interviews with experts (semi-structured). This method has limitations based on its retrospective nature.
- Think aloud protocols during task execution. Experts verbalize the knowledge and processes they are using to accomplish the task. This method is based on introspection which can interfere with task execution, especially if the task has a significant cognitive component.
- FLEX: Flexible Method of Cognitive Task Analysis. An interview-based problem-solving approach that allows capture of existing knowledge and facilitates creation of new knowledge and concepts.

Virtual environments have great potential to provide a rich, authentic practice environment that is closely matched to the operational environment along dimensions related to the learning objectives (Lane & Johnson, 2009). The virtual environment becomes a virtual *learning* environment once provisions are made to provide learners with guidance and feedback on their performance. This can be done manually by an instructor or such functions can be implemented with technology to operate seamlessly within the environment. For example, scenario selection and manipulation can be automatically driven by the learner's performance. Such supporting technologies will be discussed in more detail in Section 4.2.

3.4 Evaluation: Multiple Perspectives

The final phase of any instructional design cycle involves evaluation (although various forms of evaluation can be implemented throughout the cycle as part of an iterative design process). To assess efficacy of an instructional system, two very different types of evaluations are needed to capture both the usability of the system and its ability to support the learner (Salomon, Perkins, & Globerson, 1991).

3.4.1 Types of evaluation

An "effects of" or "summative" evaluation provides global and summary information about the instructional utility of the system as a whole. Such evaluations focus on changes in learners' understanding after they have used the system. Traditional methods for doing "effects of" evaluations include pre and post testing, and controlled studies where comparisons are made between learning with and without the system, or with different instantiations of the system. Such evaluation methods allow one to make general conclusions about the effectiveness of the instructional system.

An "effects with" or "formative" evaluation provides local information about how learners interact with various features of the system. Such evaluations provide much richer information than "effects of" evaluations and therefore help create a more detailed profile of system use. There are a variety of techniques used to gather this type of "effects of" information but most have an observational aspect. Developers may ask learners to think aloud as they interact with the system or view video of learners in an attempt to understand the conditions leading to impasses and how any provided assistance was used by the learner. Evaluation methods can also focus more directly on specific supports provided by the system to assess their usability and utility to the learner.

Kirkpatrick's model of training evaluation (Kirkpatrick 1976; Kirkpatrick 1996) includes four distinct levels, each of which provides very different information about the training system and is progressively more complicated and expensive to conduct. Level 1 is Reaction. The goal of this level is to obtain trainees' reactions to different aspects of the training system. This level is basically a measure of customer satisfaction but can also include more detailed information about components of the system. Level 2 is Learning. The goal of this level is to measure the knowledge and/or skills acquired by the trainees. This level is essentially a measure of the training effectiveness with respect to the learning goals or an "effects of" evaluation as described above. Level 3 is Behavior. The goal of this level is to measure the extent to which trainees' on-the-job behavior changes as a result of training. This level is essentially a measure of knowledge and/or skill transfer. The final level is Results. The goal of this level is to measure the overall results of the training. This level tends to focus on high-level objectives such as increased productivity or reduced costs.

3.4.2 Performance measurement and assessment

In order to be effective, the virtual environment must not only provide frequent practice of the targeted skills (accomplished through identification of learning objectives, selection of instructional strategy and scenario development), but also provide the learner with feedback on performance. Providing feedback requires performance measurement and assessment. Assessment involves applying a performance standard to a performance measurement (e.g., scoring 78 points, 8 points above the 70 required to demonstrate proficiency). The performance measures resulting from Milham et al.'s (2009) HPRA provide the information by which performance can be assessed and diagnosed, and feedback can be provided to the learner. The information gained from the learner's performance can then be used to determine the amount of practice that is needed, identify deficient skills and select scenarios to address them, and provide the content for feedback to the learner.

Recall that performance measures should flow directly from specification of learning objectives. The specification of tasks during the analysis phase of instructional design should include information about the conditions and standards for performance (Cannon-Bowers & Bowers, 2009).

A number of important factors must be considered for every performance measurement (Freeman, Stacy, & Olivares, 2009):

- The agent associated with the measured performance. The agent is essentially the source of blame for poor performance, and the recipient of feedback to improve performance. In most cases the agent will be the learner, but it is possible for the observer to have made a poor observation, or for a synthetic agent to have performed incorrectly (thus providing the learner with an inaccurate cue).
- The performance context, i.e., the setting in which the performance takes place. In a complex, realistic environment, there are many factors affecting the learner's performance. Accurate diagnosis of performance requires a thorough understanding of the conditions under which the learner acted.
- The performance data, i.e., the observations of the action. The data may come directly from the learner (survey), from the simulated environment (simulation network traffic) or may come from an observer (subjective or objective ratings).
- The measure that puts the data on a scale. Scales may be categorical (nominal or ordinal) or continuous (interval or ratio).
- The performance standard that includes a meaningful scale to facilitate interpretation.

Another important aspect of performance measures is whether they are outcome or process measures. Outcome or end state measures are sometimes referred to as measures of effectiveness (MOE) and describe *what was done*, e.g., successfully preventing enemies from reaching base in a tactical exercise. Process measures capture the steps that were taken to achieve an outcome and are often referred to as measures of performance (MOP) and describe *how things were done* (Freeman et al., 2009). In the tactical exercise example, a process measure might be the number of clear avenue of fire violations committed or closest distance achieved by enemy. An outcome or process measure can then be judged relative to some criterion as an evaluation of performance. Judging a measure to be an outcome or process measure depends critically on the training objectives, and each type of measure provides very different information about the learner's proficiency.

Virtual environments tend to be complex and rich enough to support both teams and individuals. Hence, any performance measures will need to distinguish accordingly. In cases where multiple learners are jointly participating in a scenario, each learner will have a different role, background and duty position. It is common in team exercises to have competing learning objectives, i.e., each learner's actions affect the context of other learners' actions. In cases where multiple learners are acting as a team, it can be useful to examine both team and individual performance. It is in such cases where the agent and performance context are especially important for the interpretation of performance data.

There are a variety of ways to obtain performance measurement data in a virtual environment. Subjective measures can be obtained directly from the learners. Objective measures can be provided by expert observers or collected automatically from the virtual environment using special instrumentation.

In complex environments where task execution requires input from a number of individuals, it is important to be able to distinguish between the performance of individuals and that of teams. Knowledge elicitation methods like Pathfinder and Air Superiority Knowledge Assessment System (ASKAS) have been used to examine changes in an individual's knowledge in air combat training and other military contexts (Gualtieri, Burns, Phipps, Reeves, & Pierce, 1998; Rowe, Gehr, Cooke, & Bennett, 2007; Schreiber, DiSalvo, Stock, & Bennett, 2006; Schvaneveldt, Tucker, Castillo, & Bennett, 2001). Other research focuses principally on team performance (Cannon-Bowers & Salas, 2001; Cannon-Bowers, Salas, & Converse, 1993; Cooke, 1999; Cooke, Kiekel, & Helm, 2001; Cooke & Gorman, 2006; Cooke, Gorman, & Rowe, 2009; Cooke, Gorman, & Winner, 2007; Espinosa et al., 2002; Klimoski &

Mohammed, 1994; Mohammed & Dumville, 2001). Not surprisingly, team performance research has focused on issues unique to an assessment of teams, such as knowledge distribution across team members (e.g., Cooke, Salas, Cannon-Bowers, & Stout, 2000). Combined, research on the performance of teams and individuals has suggested a variety of methodologies to use within a virtual learning environment, such as checklists, frequency counts, rating scales, and behavioral observation scales (Krokos, Baker, Alonso, & Day, 2009).

There are computational performance assessment systems that can track performance of both teams and individuals in near real time. An example is the Performance Evaluation and Tracking System (PETS) used to assess training effectiveness within Distributed Mission Training (DMT) environments (Schreiber, Watz, Bennett, & Portrey, 2003). PETS measures are derived from MECs, hence, PETS performance data can be used to quantify: (1) training effects relative to specific MEC skills, and (2) rates of improvement on these skills. Another example is the Combined Air Operations Center Performance Assessment System (CPAS) (Ockerman, Case, Koterba, Huguenin, & Garcia, 2008). CPAS captures data related to dynamic targeting linked to events in the AOC. CPAS provides the capability to augment instructor training. It is designed to store data related to events and decisions and to process data relative to a process model developed by SMEs. PETS and CPAS, *appropriately modified*, are candidates for incorporation into a performance assessment system for a virtual learning environment.

Measures of a team's performance may not be sufficient to diagnose errors. Team situation awareness (TSA) has been shown to directly impact performance, and as a result has garnered a significant amount of interest as a performance measure (Bolstad & Endsley, 2003; Cooke, Stout, & Salas, 2001; Costello, Strater, Bolstad, Cuevas, & Endsley, 2006; Gorman, Cooke, Pederson, Connor, & DeJoode, 2005; Riley, Endsley, Bolstad, & Cuevas, 2006; Salas, Prince, Baker, & Shrestha, 1995; Stanton, et al., 2005). A review of this literature reveals diverse opinions about a number of topics, including the definition of TSA, the appropriate level of objectivity for measures, and whether obtrusive measures are acceptable (Bolstad & Endsley, 2003; Cooke, Stout, & Salas, 2001; Ehrlich, Knerr, Lampton, McDonald, 1997; Flach, 1995; Gorman, Cooke, & Winner, 2006; Riley, Endsley, Bolstad, & Cuevas, 2006; Uhlarik & Comerford, 2002). TSA measures can be used to detect increased awareness during the learning process. Riley, Kaber, Sheik-Nainar & Endsley (2009) have identified the following types of SA measures:

- Direct, objective measures, e.g., SAGAT (Situation Awareness Global Assessment Technique)
- Direct, subjective measures (self- or observer- rated)
- Process measures that involve inferring SA from eye movements, verbal protocols, or team communications
- Behavior based methods that assess SA in terms of appropriateness of trainee actions to particular scenario events
- Performance measures that infer SA from situation outcomes

Performance assessment is a crucial step in the instructional design process. If directly linked to learning objectives, performance measures can provide summative evaluation information about the efficacy of the experience, and can also be used to provide instructional feedback to the learner about the details of his/her performance as an individual or as a team.

4 Considerations for Implementation in a Virtual Environment

A prevalent finding in the literature is that practice alone does not result in effective learning. Therefore, simply building a virtual environment that replicates the operational environment is not

sufficient for learning (Milham et al., 2009). A virtual environment only provides learners with practice, but no guidance or feedback. Virtual environments (and simulations) are merely tools that *can* be used to support learning. Hays (2006, p 232) points out five advantages of using virtual environments to support learning:

1. Instructional simulations are likely to have greater availability when compared to using actual equipment that may be unavailable due to other commitments.
2. Simulations can be run faster than actual equipment because simulated exercises can be reset and rerun very quickly (for example, when training air traffic controllers, simulated aircraft or other simulated entities can be quickly added or removed from instructional scenarios).
3. Simulation scenarios are reproducible, so they can be used to teach lessons that require repetition.
4. Simulations can provide the learner with more trials in a given amount of time by eliminating tasks that are not central to the instructional objective. For example, if the objective is to train in-flight refueling, the simulation can omit takeoff or landing tasks.
5. Simulations can provide the learner with cause-and-effect feedback almost immediately, when it is most effective.

A virtual environment must be enhanced so that it can make use of performance measurement information to implement instructional strategies to provide essential guidance and feedback to the learner. Only a virtual environment that is enhanced with instructional elements can enable learning (Singer & Howey, 2009). The remainder of this section will refer to a virtual *learning* environment as one which has been instructionally enhanced.

The process of creating a virtual *learning* environment requires making a distinction between task fidelity and learning requirements (Singer & Howey, 2009). Task fidelity is an important consideration for replicating the environment in which learning will occur (see Section 4.1). Learning requirements are an important consideration for enhancing the virtual environment to enable performance measurement, guidance and feedback (see Section 4.2). In some cases the enhancements of the environment may actually change the operational fidelity to achieve the instructional effect.

4.1 Central Components of the Virtual Environment

The virtual environment needs to replicate the real work environment (with sufficient fidelity) so that learning can take place in context (see Section 3.2.3). Shadrick and Lussier (2009) caution not to attempt to completely duplicate the real environment. The higher the fidelity of the simulation, the stronger the assumption that training in the virtual environment will be effective and will transfer to the real environment, but there is little empirical evidence to back this up. The required fidelity depends crucially on the learning objectives (Stout, Bowers & Nicholson, 2009). The virtual environment only needs to replicate the “what” and “how” as revealed during the task analysis (Singer & Howey, 2009).

There are many different types of fidelity described in the literature and just as many definitions. Most discussions of fidelity are grounded in the domain of combat flight training, but the underlying concepts translate nicely to the less physical domain of cyber operations.

- **Objective fidelity** (Bürki-Cohen, Soja, & Longridge, 1998; McCauley, 2006) describes how close the simulated environment models the actual operational environment.
- **Perceptual fidelity** (Bürki-Cohen, Soja, & Longridge, 1998; McCauley, 2006; Bürki-Cohen, Sparko & Go, 2007) describes the match between one’s subjective perception of the simulated

environment and the operational environment, but also between one's performance in the simulated environment and the operational environment (Bürki-Cohen, Soja & Longridge, 1998).

- **Physical fidelity** (Andrews, Carroll, & Bell, 1996) or **environmental fidelity** (Menaker, Coleman, Collins, & Murawski, 2006) describes the physical layout of the simulated environment and its match to the operational environment.
- **Functional fidelity** (Andrews, Carroll, & Bell, 1996) describes the way the simulated environment operates compared to the operational environment, and can be much more important to learning than physical fidelity (Shadrick & Lussier 2009).

Drawing on experiential learning literature, Menaker et al. (2006) introduce the notion of '**cognitive fidelity**.' They emphasize the importance of distinguishing between the physical environment in which learning takes place, and the cognitive tasks in which the learner engages. They "fear that the pendulum has swung to the physical fidelity because technology enables us to create more realistic environments, often at the expense of the cognitive fidelity… (p. 3)." It may not be necessary to replicate all aspects of the task environment to facilitate learning, and in some cases, high environmental fidelity can actually contribute to cognitive overload which can detract from learning.

An important goal of instructional design should be finding the optimal balance of environmental and cognitive fidelity to maximize learning and transfer to the operational environment. It may be useful to incorporate higher levels of environmental fidelity as learners gain experience and are able to distinguish between information that is essential and extraneous to their tasks. We need to understand the perceptual and cognitive experiences that the simulator needs to provide to support performance that will generalize to the operational environment (Tsang & Vidulich, 2002). Although a training environment may be physically similar to the operational environment, the fundamental human interaction with the environment (the cognitive activity) can be very different (Chung, 2000).

Simulation designers and engineers have attempted to replicate as many physical and functional stimuli as possible in the training environment, but these efforts are thwarted by three important factors (Andrews, Carroll, & Bell, 1996):

- The inability to specify the kinds of stimuli required for a particular task. Recent cognitive approaches (e.g., task analysis methods) take into account an understanding of how humans learn and perform which goes well beyond the previous analyses based on stimulus-response conditions. There is also better understanding of human perceptual system which helps specify how cues are recognized and processed.
- Technological difficulty replicating some stimuli. Great advances in technology have brought forth a host of sophisticated network capabilities.
- Cost of replicating stimuli. As technologies advance, prices do come down but cost will always be an important factor.

Since it is not possible to replicate all of the stimuli present in the real-world environment (even if technology and cost were not factors), Andrews, Carroll, and Bell (1996) suggest choosing to simulate only those stimuli that are necessary to perform the task and refer to this as **selective fidelity**.

Jones, Hennessy and Deutsch (as cited in McCauley, 2006) make the following conclusion about fidelity which sums up the literature quite nicely:

> "The purpose of a simulator is to provide the conditions, characteristics, and events present in the operational situation necessary for the learning of skills that will be performed with actual equipment… Two related principles derive from this premise. First, the characteristics and methods of using simulators should be based on their

> behavioral objectives. Second, physical realism is not necessarily the only or optimal means for achieving the behavioral objectives of simulation. Because the history of simulator development is characterized by striving for improved realism through the advancement of technology, it is easy to forget that the learning or performance—not physical duplication—is the primary goal (p. 28)."

Most VEs aim to replicate a physical environment and include important subsystem components such as position tracking, visual displays (head-mounted and/or projector-based), and multimodal displays (e.g., haptic, olfactory, vestibular). Due to the electronic nature of the cyber domain, the VE need not have the same physical fidelity as VEs for other domains. Instead, the central components of the VE will be focused on replicating the information environment, i.e., the networks, systems, and displays.

One particularly important element for inclusion with cyber-related VEs is the representation of capabilities from other domains which may have effects in the cyber domain (Jabbour, 2009). Jabbour states "Integrated effects modeling, simulation, and war-gaming must include the integrated delivery of effects from blue and red systems in every domain against red and blue systems in every domain. Integrated effects exercises must provide a realistic environment for cross-domain operations, in which activities in one domain have a direct bearing on activities in another" (p. 13).

Innovative visualization, "a graphical representation of data or concepts" (Ware, 2004, p. 2), is perhaps the most essential element for the cyber VE. Cyber operations are unique in that only top-level outcomes are typically observable, while the underlying processes are not directly observable (Zacharias, 2009). It is the underlying causes that must be targeted in any cyber-relevant effort. This poses problems not only for learning how to counter such attacks, but also for actual operations.

Visualization has been characterized as a general method or tool used in situations in which large amounts of complex data must be transformed and represented in a meaningful way for comprehension (see Kocka & D'Amico, 2004; Lengler & Eppler, 2007; Robertson, Czerwinski, Fisher, & Lee, 2009; Thomas & Cook, 2005). According to Ware (2004), effective visualization is beneficial in several ways; it facilitates comprehension of large quantities of data, discovery of high level patterns or emergent phenomena in data, detection of problems in a data set, understanding of relationships between local and global relationships, and hypothesis formation. Design of visualizations should be informed by the field of cognitive informatics, which looks at the relationship between information processing mechanisms in the brain (including perception and inference), the underlying structure of the knowledge, and its processing in computational environments (Wang, 2007; Yao, 2004).

Recent efforts have employed visualizations to represent mission critical function status. For example, work has been conducted for AMC to effectively present alerts related to emerging problems that threaten the viability of a mission (Wampler et al., 2005). Efforts are currently underway to apply visualization in this manner to help the AMC develop candidate TTPs to effectively counter cyber attacks within the context of special assignment airlift missions (E. Kean (AFRL/RISA), personal communication, April 12, 2010). Similarly, systems in development are utilizing visualization to display the mapping of mission critical functions to likely future states of the system, given information about the types of plausible cyber attacks against that system (Salerno, 2008; Tadda, 2008; Salerno & Tadda 2009; Holsopple et al., 2009). Visualization of spatial and temporal patterns has been used in the area of cyber security (Ma, 2004; Hideshima & Koike, 2006). For example, D'Amico and Larkin (2001) designed visual representations that convey information security events over time and depict the impact of security breached on mission-critical tasks.

As mentioned previously, it is important to clearly separate the fidelity of the environment from the instructional enhancements that make it a virtual learning environment (Singer & Howey, 2009). The

essential use of visualizations in a cyber VE is a perfect example of how simply duplicating the operational environment could impede learning. Innovative visualizations will not only support learning, but are also essential enablers of cyber-relevant skills. The processes underlying cyber attacks must be made visible to help teach airmen how to recognize them, defend against them, and fight through them. Visualizations developed for a cyber VE may actually inform the need for new operational displays or procedures. Once the required fidelity and essential components of the virtual environment have been established, efforts can be directed toward the development of technologies to support learning.

4.2 Supporting Technologies

This section will discuss the supporting technologies needed to create a virtual *learning* environment, increasing the training value of a virtual environment. The essential components of the environment (Section 4.1) merely replicate the task environment and provide a context in which learning can occur (Cannon-Bowers & Bowers, 2009).

As mentioned in Section 3.2.4, guidance and feedback are the most essential component of any learning environment, virtual or otherwise. By their very nature, rich virtual environments support the acquisition of complex skills. Ritter and Feurzeig (as cited in Lane & Johnson, 2009) point out that the complex knowledge acquisition process complicates performance assessment, error diagnosis and delivery of feedback. Expert performance involves compilation of knowledge for efficiency and performance would suffer from interruptions for guidance or feedback.

Although a virtual learning environment could benefit greatly from advanced instructional technologies such as instructor-operator stations or scenario authoring and management tools, we suggest that *the most critical supporting technologies must focus on the delivery of guidance and feedback to the learner (enabled by performance assessment)*. Shadrick and Lussier (2009) reiterate this need calling for "performance measurement to assess whether the task is performed correctly, active and effective coaching, opportunity for immediate repetition of poorly performed tasks, and focus on tasks that are difficult, critical, or constitute areas of individual or collective weakness".

Ritter and Feurzeig (as cited in Lane & Johnson, 2009) suggest three ways to provide guidance and feedback: Before practice (e.g., demonstrations of expert performance), during practice (e.g., coaching supports), or after practice (e.g., after-action review). We focus our discussions on means by which guidance and feedback can be delivered during and after practice using a virtual environment.

4.2.1 Delivering guidance and feedback during practice

A defining characteristic of intelligent tutoring is its delivery of individualized feedback to the learner (see Section 3.2.2). Rickel and Johnson (1997) were the first to propose the use of intelligent tutoring techniques in virtual environments, noting novel methods of interaction afforded by the virtual environment. Lane and Johnson (2009) also tout the benefits of virtual environments for learning because of the increased scope of tutorial interactions that are possible. This is in part due to the variety of means by which feedback can be delivered and the bandwidth available for monitoring the learner's performance.

Lane and Johnson (2009) have defined two fundamentally different approaches for providing guidance and feedback in a virtual environment. (1) Experience manipulation involves the amplification of and dampening of implicit feedback within the virtual environment. Implicit feedback often mirrors the cues that are present in the real environment, e.g., display messages or alarms. Adjusting the behavior of virtual environment elements to achieve an instructional objective can often be in conflict with the goal of maintaining fidelity of the environment (Wray et al., 2009). (2) Stealth tutoring approaches deliver

more explicit guidance and feedback (e.g., tutor-like messages), but do so through an element of the virtual environment rather than through an explicit tutor entity (e.g., through another character in the scenario). Wray et al., add dynamic tailoring as a third approach for providing guidance and feedback in a virtual environment. Dynamic tailoring requires continuous adaptation of the environment through learners' interactions with the on-going scenario. This approach truly individualizes the learning experience by providing support, fading support, and challenging the learner at appropriate times. In all these approaches, the guidance and feedback is carefully faded so that the learner does not become dependent on the assistance and is ultimately able to perform independently.

Singer and Howey (2009) provide an alternate framework to conceptualize the enhancement of a virtual environment to support learning. They propose the use of augmenting cues and adjuncting cues, both of which involve deviations from fidelity. An augmenting cue is similar to Lane and Johnson's (2009) experience modification. The characteristics of stimuli that are normally present in the real environment are altered to enhance their salience (or the salience of surrounding/interfering cues are decreased). This approach to guidance requires careful selection of the cues that are critical to task performance. An adjuncting cue is a more explicit form of guidance and feedback. Discriminative cues are added to the virtual environment (e.g., pointing or actual coaching instructions). This approach requires that learners understand the role of the additional stimuli, and do not confuse them with naturally occurring cues that must be attended to in the real environment. Fading is particularly important in this approach. Lintern and Roscoe (as cited in Singer & Howey, 2009) point out that such cues can simplify a task considerably, allowing the learner to converge quickly on the correct control responses, but gradual withdrawal of the supplementary cues are needed to force the trainee to become increasingly dependent on the cues that are normally available.

Agent-based technologies have been used to realize a range of guidance and feedback in instructional systems. A software agent is simply a software system designed to interact (perceive and act) within an environment, which could be a physical environment (i.e., a robot) or a virtual environment (e.g., a computer game "bot"). Pedagogical agents provide explicit guidance in a learning environment (Rickel & Johnson, 1997). The instructional efficacy and power of using such agents in knowledge-based learning environments has been repeatedly demonstrated (Johnson, Rickel, & Lester, 2000; Moreno, Mayer, & Lester, 2000; Lester et al., 1997; Lester, Converse, Stone, Kahler, & Barlow, 1997).

Lane and Johnson (2009) identify two possible roles for pedagogical agents in virtual learning environments. The agent may act as an actual coach or tutor in the environment. This approach is consistent with Singer and Howey's (2009) adjuncting cues or Lane and Johnson's (2009) stealth tutoring approach. It may be appropriate for some training but it has the serious drawback of compromising the realism of the environment and interfering with learner performance. The agent may also assume a role in the underlying scenario, playing out details to accomplish instructional objectives and tailor the scenario to the learner's needs. This approach is consistent with Singer and Howey's (2009) augmenting cues or Lane and Johnson's (2009) experience modification approach.

Guidance and feedback are essential to the learning process and must be incorporated into any virtual *learning* environment. The above approaches outline some of the many ways this can be accomplished.

4.2.2 Delivering guidance and feedback after practice

After-action reviews (AARs) are another way to provide learners with the guidance and feedback critical for learning and skill acquisition. The military has embraced this idea by instituting AARs as a foundation of modern military training. In AAR, trainees and instructors discuss what happened, why it happened, and how to improve performance in the future. The efficacy of AAR discussions depends critically on the focus of discussions. They must be based on precise information about what took place during practice

(not just participant's impressions or recollections), and they must also be focused on the instructional objectives.

Lampton, Martin, Meliza, and Goldberg (2009) summarize the two distinct forms of feedback that can be provided during AAR. Intrinsic feedback is based in perceived truth, i.e., the cues that participants perceive about their own performance, from their own perspective in the scenario. Extrinsic feedback is based in ground truth, i.e., the actual sequence of events that took place during the scenario. Often the ground truth information is not readily available for AAR, but in a virtual learning environment (instrumented with appropriate tools), this information can be made available to guide AAR discussions. Playback capabilities, or views from different perspectives, can allow demonstration of ground truth.

Implementation of effective AAR for a virtual learning environment must take into account both the learning objectives and learners' performance in the scenario. Access to this information will require supporting technologies to be integrated into the virtual learning environment, but will provide a valuable instructional support.

Appendix D includes a survey of existing cyber simulations and technologies, outlining their capabilities as central components of a VE and identifying gaps to be addressed so that learning is better supported (i.e., so that they may be used as VLEs).

4.3 Guiding Design Concepts

The development of any virtual learning environment will naturally require the design of systems, displays and interfaces with which learners and instructors will interact. Learners will interact primarily with the essential components of the system as they perform tasks, but also with the supporting technologies that will provide guidance and feedback during the experience. Instructors may also interact with the supporting technologies as they develop training scenarios, observe learner performance, or provide feedback. Adherence to research-based design guidelines will help to ensure that the learners' and instructors' experiences can be focused on the learning objectives, and not hindered by deficiencies in the environment. The following sections outline some design guidelines from the fields of human factors and usability.

4.3.1 Human factors considerations

As mentioned in Section 2.3, the field of human factors focused on the human's capabilities, limitations, and expectations with respect to the design of systems and tools. Learner-centered design (LCD), user-centered design (UCD), work-centered design (WCD), and human-centered design (HCD) are all human factors approaches that aim to create effective and efficient interactions between the human and the technological systems with which he/she works.

LCD (discussed in Section 3) focuses on the human as a learner, a novice who needs support as he/she learns to perform new tasks. UCD on the other hand focuses on a knowledgeable user and ways to facilitate the user's execution of various tasks. A traditional UCD approach is used to assist users in their work (Norman, 1986). The target audience (the user) already understands the basics of the work practice but needs a tool to help them complete their work more easily and effectively. The user is not necessarily trying to learn about their work through use of the tool. The design process must address the conceptual gulfs between the user and the technology (Quintana, Krajcik, & Soloway, 2001, 2003). More specifically, the execution of actions must be straightforward and consistent with the user's goals, and the evaluation of the state of the technologies and systems must be understandable by the user. These usability issues tend to be the primary focus of UCD.

The key elements of WCD (Eggleston, Roth & Scott and Roth, as cited in Roth et al., 2006) are: the analysis and modeling of the demands of the work, the design of displays and visualizations that integrate data into meaningful information in the context of the work, and use of evaluations that probe the ability the system to support the work across a representative range of work context and complexities. Effective WCD results in usability, but also usefulness (the extent to which it facilitates work performance), and impact (the extent to which it supports work the individual's work goals and those of the individual's team and organization) (Roth et al., 2006).

HCD incorporates the user's perspective into the actual software development process. This is especially important when multiple users utilize the same system or tool for different purposes, as the design must account for the various needs. The key principles of HCD are (Maguire, 2001): Active involvement of users and clear understanding of the user and task requirements, appropriate allocation of function between the user and the system, iteration of design solutions, and multi-disciplinary design teams. In HCD, scenarios of use are an integral part of the design process as they exemplify the user needs and contexts of use.

Regardless of the type of design employed, it is imperative that the user (learner or instructor), user's needs, user's tasks, and available tools are taken into consideration. A virtual learning environment will include a variety of systems and tools, and is likely to be designed to address the learning objectives of multiple groups. The concepts of LCD, UCD, WCD, and HCD can provide valuable insight to inform the design and effective use of virtual learning environments.

4.3.2 Usability

The virtual learning environment, must not only address the needs of its users (learners or instructors). It must also be genuinely usable. A truly usable system has a number of important benefits (Maguire, 2001): Usable systems result in increased productivity, reduced errors, reduced training and support, improved acceptance and enhanced reputation. Usability ensures that users are not distracted or hindered by the system, and can concentrate their efforts on using the system for its designed purpose.

As various systems, tools, and technologies are developed as part of a virtual learning environment, it is important to ensure their usability. Heuristic evaluation is a diagnostic usability inspection method used to provide quick and inexpensive feedback on an interface design. A small set of evaluators play the role of an inexperienced user and judge the system's compliance with guiding principles of usability (the heuristics). As heuristic evaluation is intended to be an integral part of an iterative design process, it not only identifies usability problems but also provides recommendations for addressing them.

The heuristics used to guide an evaluation (and ultimately the design) are central to the utility of the results. Nielsen (1994) developed the following ten usability heuristics to be guidelines for interface design. Nielsen's heuristics are used as the basis of many interface evaluations.

1. **Visibility of system status**: The system should always keep users informed about what is going on, through appropriate feedback within a reasonable time.
2. **Match between system and the real world**: The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
3. **User control and freedom**: Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.

4. **Consistency and standards**: Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
5. **Error prevention**: Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
6. **Recognition rather than recall**: Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
7. **Flexibility and efficiency of use**: Accelerators -- unseen by the novice user -- may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
8. **Aesthetic and minimalist design**: Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
9. **Help users recognize, diagnose, and recover from errors**: Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
10. **Help and documentation**: Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

5 Science & Technology Recommendations

The previous sections have described the cyber domain, theory and methodological approaches focused on the joint optimization of human performance and technology, and findings from literature pertaining to instructional science. The instructional focus of the S & T plan was motivated by numerous factors, including requirements submitted by AFSPC and USSTRATCOM as well as the findings of the USAFSAB studies (as discussed in Section 2.5.1). The reviews conducted under this effort indicate that application of instructional S & T efforts will benefit a number of mission critical functions including enterprise-level computer and network security operations, C2 operations for air and space (AOC), air mobility operations, and ISR operations. Section 5.1 will identify a number of general instructional S & T recommendations based on the instructional literature summarized in Sections 3 and 4. These recommendations are applicable to each of the selected mission critical functions. Section 5.2 provides an example of how these recommendations can be applied to one of the mission essential functions – C2 (AOC) for air and space.

The goal of the instructional recommendations is to inform the development of advanced instructional technology for individuals and teams. Implementation of these recommendations will support operational readiness for mission assurance, with a focus on detection, assessment, response, and recovery from cyber exploitation, attack, and malicious manipulation. These recommendations are intended to facilitate the development of advanced skills, situation awareness, and complex decision making in Airmen.

5.1 Instructional S & T Recommendations

The following recommendations are derived from instructional theory and are essential for the development of effective VLEs to prepare Airmen to operate in contested cyber environments. As noted by the USAFSAB (2008), cyber-relevant TTPs for mission essential functions including C2, air mobility operations, and ISR operations are less developed than those for enterprise-level computer and network security operations. Accordingly, the development of TTPs may be occurring simultaneously with the implementation of these recommendations. TTP development will be informed by the determination of plausible cyber attacks, their effects on information technology and networks, and, ultimately, estimates of their effect on mission operations. Assessment of the effects of attacks on networks and technologies for various mission critical functions may rely on the use of cyber ranges and, to some extent, analytical simulation. A mechanism should be enabled to ensure that TTP development efforts, as completed by the appropriate military experts, iteratively inform and shape the implementation of the following recommendations.

1. **Specify learning objectives.** Effective individual and team training for cyber threats requires learning objectives focused on detection, assessment, response to, and recovery from cyber exploitation, attack, and malicious manipulation. Learning objectives are likely to be tightly tied to emerging TTPs, and are an essential first step in instructional design (as summarized in Section 3). The MEC process, as described in Section 3.1.2, may be utilized to identify relevant individual and team competencies, thus informing the development of learning objectives that will help to prepare Airmen to respond to cyber threats. Existing cyber-relevant TTPs may also be referenced to support learning objectives formulation.

2. **Develop a realistic environment.** To maximize learning and support transfer of learning to the operational environment, VLEs must represent the essential systems, processes, and context of the operational environment. As discussed in Section 4.1, the levels of objective, perceptual, physical, functional, and cognitive fidelity of a VLE are important considerations. The required levels will depend on many factors including the targeted group of learners. Instruction for cyber attack detection by Airmen conducting C2 functions may require only the presentation of attacks' effects, whereas detection opportunities for enterprise-level computer and network security operations personnel may require a more precise level of environmental fidelity. In the former case it may also not matter whether network components (e.g., routers, computers) are simulated or virtualized, but it will in the latter. Lastly, cyber effects resulting from capabilities in other domains should be incorporated to enable a realistic context for instruction.

3. **Develop realistic scenarios.** Instructional scenarios must represent the effects of plausible cyber attacks on information technology and networks represented in the VLE. Scenarios for use in the VLE should also include appropriate triggers to elicit the behaviors specified by the learning objectives.

4. **Use visualization to support learning.** As discussed in Section 4.1, the cyber-relevant instruction could benefit greatly from the use of visualization to make visible underlying processes and system states that are currently not observable. Making this information accessible would not only facilitate learning during scenarios, but also in AAR.

5. **Develop automated performance measurement capability.**

    a. Automated performance measurement at both the individual and team level is needed to support the delivery of feedback to the learner (either during or after practice, as described in Section 3.2.4). Practice without feedback is unlikely to result in learning. The use of agent

technology to provide instructional guidance and feedback would require detailed performance information. This proven approach to instruction can then be utilized in an active, coaching/tutoring capacity or as a less explicit capacity (see Section 4.2.1), to provide instruction that is adapted to learner needs.

   b. Evaluation (Section 3.4.1) is another important component of the instructional design process, and performance measurement information (based on learning objectives) can be used to evaluate the efficacy of instruction and the transfer of skills to the operational environment. Controlled experiments should be conducted to assess efficacy and transfer. The costs associated with any particular VLE will need to be evaluated with respect to the benefits (effectiveness of training and transfer of skills and knowledge to the job).

6. **Develop AAR capability.** Technology is needed to support after-action review for centralized or distributed training. This technology, as discussed within Section 4.2.2, should facilitate post-exercise discussion of the execution errors, lessons learned, and other considerations noted during scenario play. AAR technology should provide access to ground truth, relieving instructors and trainees of some amount of effort required to manually reconstruct these events. By addressing some of the needs for reconstructing events, AAR capabilities can increase the amount of time instructors and trainees have to discuss the scenario events and their meaning.

7. **Develop scenario authoring capability.** Technology is needed to facilitate training exercise scenario authoring, as noted in Section 4. Distinct from scenario development capabilities, scenario authoring capabilities refer to the technical ability to program a series of events and rerun them with relative ease (Section 3.3). In the case of instruction for the cyber domain, it is feasible to imagine presentation of a pre-determined string of cyber attacks or the effects of cyber attacks. The ability to manually string together scenario events is needed. Enabling instructors to modify scenarios as needed to embed the appropriate triggers for performance is essential (see Section 3.3). Virtualization-based technology may, in some cases, enable rapid reconstitution of the VLE and scenarios to support agile and less costly training.

5.2 Practice and Instructional Environment for AOC

In the previous section we summarized a number of instructional S & T recommendations applicable to a variety of mission essential functions. This section will discuss the recommendations by focusing on a particular function: C2 operations (in the AOC) for air and space.

5.2.1 Current AOC testbed

Given findings and perspectives in the USAFSAB summer studies (2007a, 2007b, 2008), from the workshop hosted as part of this effort, and from other formal activities, the AOC and its networks are a viable and important context in which to implement a VLE. The AOC is the lead C2 node in airborne networks, and is itself a hybrid mixture of communication links, hardware, and software operated by AF personnel with a variety of AFSCs. Fortuitously, an AOC-ISR testbed exists at AFRL. Also, operational and training AOCs exist in multiple locations, thus offering access to subject matter experts and operators familiar with the systems and operations of the AOC. While the AOC at Nellis Air Force Base (AFB) and Hurlburt Field are training installations, those at Davis-Monthan AFB, Hickam Field, and Shaw AFB are operational. Thoughtful coordination with personnel at these installations will facilitate the expansion of the AOC-ISR testbed in ways that support instructional research and development, as well as provide relevant and challenging training experiences for active duty personnel in the process of evaluating candidate practices and tools.

Figure 2 depicts a notional airborne network, and Figure 3 depicts Joint Communications Links for the JV 2020 System of Systems Architecture. These figures reveal several important points. First, AF networks involve terrestrial, space, and airborne assets, all of which are tethered by communications links. Second, an AOC is the hub of C2 of airborne operations. Third, execution of airborne operations depends not only upon C2 by an AOC, but also on information gathered and synthesized by intelligence, surveillance and reconnaissance activities conducted using a variety of methodologies, as well as upon airborne tactical control and support assets such as Air Battle Management (ABM) platforms, tankers, and the communication links among assets (note the partial redundancy among communication paths in Figure 3). Hence, enhancement of the AOC-ISR testbed offers multiple opportunities for future expansion to other platforms and a rich environment in which to explore the effects of cyber attacks. Accordingly, the AOC-ISR testbed at AFRL is ideal for implementation of the instructional S & T recommendations.

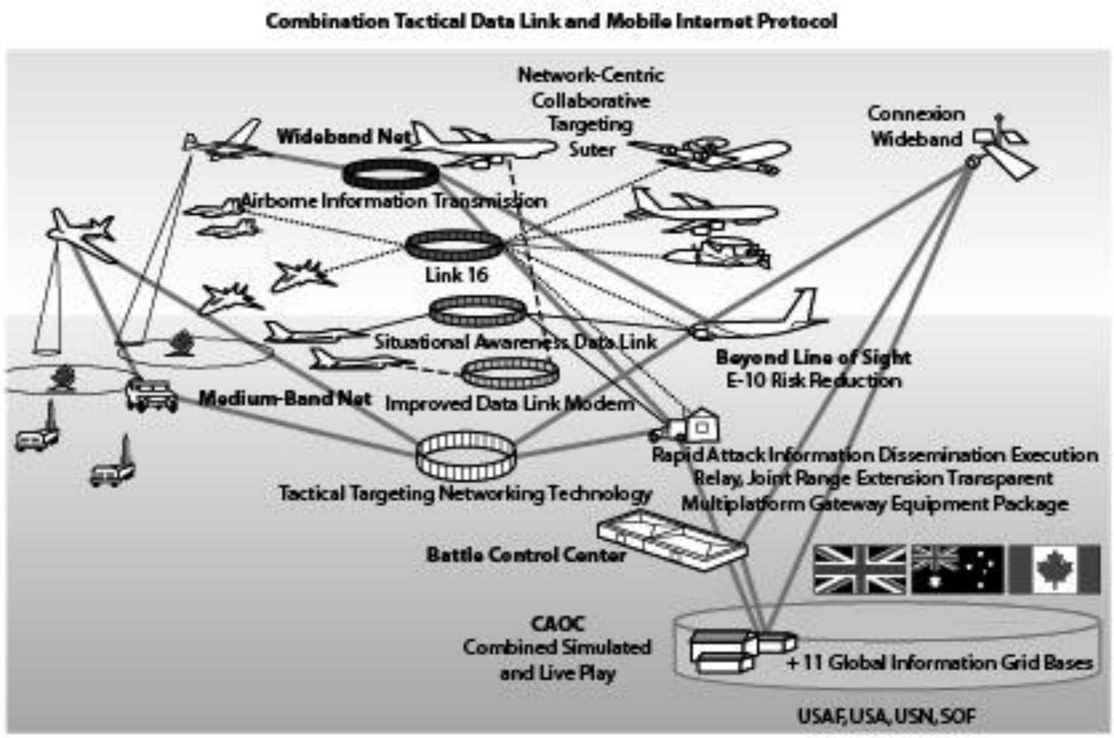

Figure 2. A notional AF airborne network

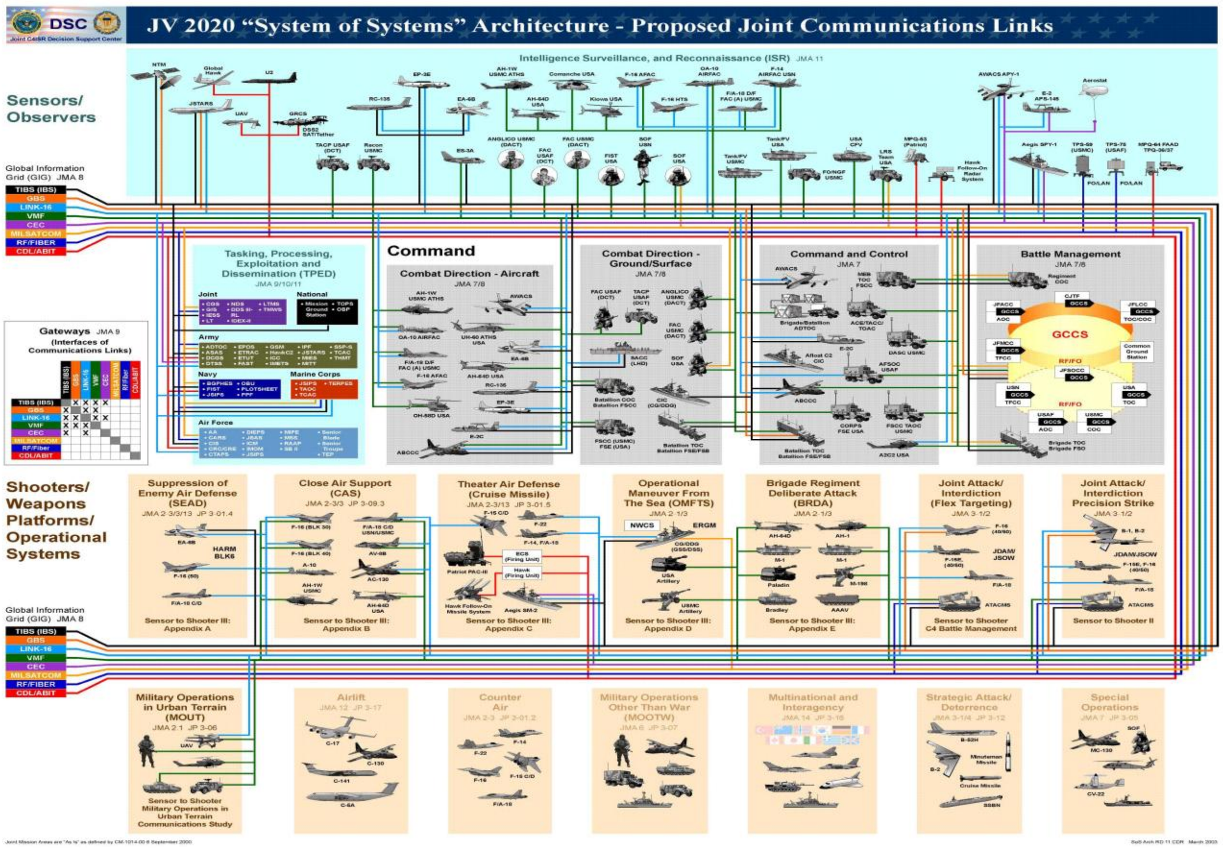

Figure 3. System of systems architecture - JV 2020 joint communication links

Technically, the AOC and ISR system is labeled the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Training and Rehearsal Testbed (C4ISR TRT). In the aggregate the C4ISR TRT system replicates a subsection of a functional AOC. The servers of the system provide modeling and simulation data to operator systems. The original concept of operations for this system was to use the C4ISR TRT and MEC processes to: (1) define AOC training requirements and provide a C2 Distributed Mission Operations training framework; (2) enhance current simulation-based AOC training or large-scale and unit training, such as Mission Qualification Training and Continuation Training; (3) develop performance-based criteria, methods, and tools for evaluating AOC operator combat mission readiness, and (4) explore and develop innovative technologies for specific AOC and ISR training need areas. The system is owned by the Air Force Research Laboratory, Warfighter Training Research Division (AFRL/RHA).

5.2.2 Near and long-term C4ISR TRT modifications

Specifically, this section will discuss required modifications to the C4ISR TRT in order to implement the instructional S & T recommendations.

As indicated in Section 5.1, the specification of cyber-specific learning objectives is an area in need of focus (see also Appendix C regarding current cyber-specific learning objectives and MEC knowledge and skills for the AOC). Given the current lack of objectives for mission critical functions including C2 (in the AOC), an expansion of the C4ISR TRT may initially serve as a pure practice environment in which TTP testing and development occur. As discussed in Section 3.3 a rich, authentic practice environment differs from a VLE in that the latter provides learners with guidance and feedback on their performance.

We recommend that the expansion of C4ISR TRT capabilities for cyber training not wait for the learning objectives to be specified. Rather, some capabilities (e.g., simulation of cyber attack effects and scenario development) may be meaningfully advanced in the near-term. This is a similar to the approach being adopted for air mobility operations, for which current efforts are focused on building an environment in which classes of cyber attack vectors may be implemented to facilitate TTP development (E. Kean (AFRL/RISA), personal communication, April 12, 2010). The recommendation to proceed with development of a practice environment should not be interpreted as a dismissal of the importance of or need for learning objectives. The learning objectives, once determined, will inform efforts related to each of the other recommendations as described in Section 5.1.

The current C4ISR TRT presents learners with a realistic context in that the testbed is representative of a baseline AOC system. However, the ability to present cyber attack signatures in the C4ISR TRT has not been enabled to date. Modification of the C4ISR TRT will require expansion to include either the capability for cyber attack generation or presentation of cyber attack effects, depending on the instructional goals. If the attack generation option is exercised, a number of currently existing threat generation systems may be evaluated for potential integration (for an evaluation of current modeling and simulation tools for cyber, see Katz, 2010). The presentation of effects option can be informed through the use of analytical simulation to determine the effects of various cyber attacks. Following documentation of the effects and signatures of cyber attacks to the systems, custom modifications would be required to enable simulation of attack effects/signatures within the C4ISR TRT.

Cyber attack or cyber attack effect simulation capability is not a complete solution to achieve a VLE. Threat simulation must occur within a rich, immersive context with appropriate triggers to elicit the behaviors specified by the learning objectives. We recommend continuation of the scientific effort at AFRL to document and archive successfully validated scenarios for future use in the C4ISR TRT. Scenarios such as those previously utilized during Training Research Exercises (T-REX) events provide a good foundation for future scenario development. A second option for generation of scenario data is to leverage data from missions previously completed by the operational community. Such an approach is being utilized currently to develop scenarios for cyber-related scenarios for air mobility operations (E. Kean (AFRL/RISA), personal communication, April 11, 2010). Data of this nature has its advantages including having baseline of performance (e.g., time to complete).

Likely cyber threats to AOC systems must be identified and should be prioritized by accepted criteria (e.g., for severity, likelihood, etc) prior to scenario development. A current Prioritized Threat List (PTL) should be developed and maintained along with known work-around solutions to specific threats. It is an assumption of this instructional S & T plan that the selection of initial threats on which to build scenarios will focus on threats that are judged to be particularly destructive and for which relevant AOC scenarios can be built. Once a PTL exists, scenario development can proceed in a systematic manner, by focusing on the highest priority cyber threats that can realistically be represented in the expanded AOC. Building and maintaining a scenario database must be an on-going effort. The AFRL should explore relations with AF and other services units, as well as certain agencies of the U.S. Government in order to identify, classify, develop, and deploy responses to cyber threats. Contacts should be maintained with personnel at training facilities (e.g., at Combined Air Operations Center -Nellis and the Formal Training Unit, Hurlburt Field) in order to coordinate efforts and share findings from research exercises. Close relations with the 57th Aggressor Squadron at Nellis AFB and with a variety of units at the 24th AF will be developed and maintained. The nature of these relations may take the form of periodic briefings, interviews with key personnel on location, or workshops conducted by team members at AFRL. The purpose of these activities will be identification and prioritization of known (and potential) cyber threats to the AOC to feed into scenario development efforts.

Initially, visualization may be utilized to inform the development of TTPs for mission assurance in the AOC. The recent efforts to identify and visualize the mapping of critical C2 systems and the likely future states of those systems as a result of cyber attacks is a valuable step toward TTP development. As noted in Section 4.1, visualization is being utilized in this fashion toward the development of candidate TTPs to effectively counter cyber attacks to air mobility operations. Similarly, systems in development are utilizing visualization to display the mapping of mission critical functions to likely future states of the system, given information about the types of plausible cyber attacks against that system (Salerno, 2008; Tadda, 2008; Salerno & Tadda 2009; Holsopple, Yang, Kuhl, Hall, Nagi, Shapiro, Sudit et al., 2009). Currently, no AAR visualization capabilities exist in the C4ISR TRT to illustrate the occurrence of cyber attacks and the corresponding effects on AOC systems and team processes and performance. Reconstruction of scenario events through the use of visualization is one option which may be explored in the C4ISR TRT.

Performance measurement and evaluation – particularly measurement that is automated and unobtrusive during training research events – is the key to understanding which mission assurance behaviors are effective and which are not. Currently, the C4ISR TRT utilizes outcome and communications-based measures of performance and process relative to current (non-cyber related) learning objectives. Current measures do not account for accuracy in detection or effectiveness of responses to cyber attacks or cyber effects at either the individual or team level. Performance measurement and evaluation capabilities will need to be closely aligned to the emerging cyber-relevant learning objectives for the AOC. C4ISR TRT expansion efforts should support engineering effort to expand current performance measurement and evaluation system to account for cyber-related elements. Once measurements are specified, engineers can work to implement automated, competency-based, performance measurement and evaluation capabilities.

There are on-going science and engineering efforts at AFRL Mesa Research Site to identify and implement automated, competency-based, performance measurement and evaluation in simulators modeling a variety of weapons platforms (e.g., Stock, Schreiber, Denning, & Cain, 2006). A review of these efforts reveals that the non-negligible, on-going costs are more than compensated for by the dividends associated with high-validity, high-specificity types of feedback available in after-action review. The creation of algorithms to compute performance measures and the associated software engineering to produce summary measurements and evaluations in near-real time (essential for maximally effective AAR) requires sustained engineering efforts. An expanded C4ISR TRT will require comparable levels of science and engineering efforts to incorporate comparable performance measurement capability. Development and engineering efforts are required to develop AAR capabilities to facilitate discussions of cyber attack-related execution errors and lessons learned.

An additional capability of the C4ISR TRT expansion should be scenario authoring. Instructors ought to be able to build scenarios to fulfill the instructional objectives. Authoring capabilities should enable instructors to program a series of events to elicit behaviors or exercise emerging TTPs. Control over the presentation of scenario events is a critical capability given that the learning objectives and TTPs will be evolving over time. Scenario authoring capability will enable the flexibility required in this type of dynamic setting. Such capability may also assist in manual (by instructor) adaptation of scenario presentation based on an individual or team's performance.

Due to the emerging nature of cyber-specific learning objectives, requirements, and technology, the development of a VLE is likely to involve multiple iterations of the recommendations described here. Once learning objectives are developed, they will inform the development of scenarios, performance assessment and AAR capabilities, and the use of visualization. Emerging threat tactics may also inform each of these topics and result in refined learning objectives.

Contemporary instructional science must persist as an essential component for the long-term C4ISR TRT expansion effort. On a regular basis, scientists and engineers should undertake efforts to remain current with these perspectives. Instructional science is constantly advancing, therefore it is important to conduct, on a periodic basis, focused reviews of the literature to retrieve and assess the latest instructional science approaches to individual and team-learning of complex skills. Such reviews will inform and support experimental training syllabi development. There is a particular need to explore the application of innovative approaches to learning (such as "pattern-matching" intuitive cognition, Klein, 2009). These approaches are most likely to have an impact on the type and frequency of training exercises.

Augmenting the need to assess instructional science advances is the equally important need to assess current doctrine relevant to AOC processes, as well as to review MEC documents to identify the current level of focus on mission assurance with respect to cyber threats, and to explore the possibilities for objective performance measurement, which is a necessary basis for effective and efficient AAR. These complement other efforts that are required to identify the mission critical functions of the AOC as it operates in airborne networks.

C4ISR TRT expansion efforts should be reviewed regularly by authorities on current cyber threats who are also familiar with AOC processes. The overall goal of this activity is to keep the AFRL team focused on: (1) improvement of instruction, (2) increasing realism in scenarios, (3) keeping in touch with activities not appearing in academic or military publications, (4) early detection of possible missteps by the AFRL team, and (4) receiving a periodic review on team instruction and evaluation efforts. This research will benefit most when systematic efforts are undertaken to empirically validate the research activities.

6 Conclusions

Although the primary concern relative to cyber threats is the protection of information systems and networked warfighting capabilities, humans play a vital role in the process and should therefore not be overlooked. Joint optimization of human performance and technological capabilities is required for effective response. The recommendations presented in this S & T plan focus on furthering advanced instructional capabilities. Such capabilities are essential for achieving mission assurance in a contested environment. We anticipate that cyber threats will escalate in times of conflict, therefore delaying the moment of judgment of the USAF's cyber preparedness until the moment when it matters most.

Preparation is required both at the individual and team levels. The instructional considerations discussed in this instructional S & T plan will enable effective and efficient preparation at these levels. Instructionally-based requirements for cyber operations VLEs will provide both practice and learning environments for warfighters in which they can develop and refine cyber defensive techniques. Due to the different systems and processes used by the military departments, there is clearly no one solution for cyber instruction and training. However, many of the instructionally-focused recommendations put forth in this plan will be applicable across military departments.

7 References and Related Materials

Air Force Communications Agency. (2007a, 5 October). Combat Information Transport System Block 30: Enabling Concept (Draft). Scott AFB, Belleville, IL: Air Force Communications Agency/Electronic Communications Network. Air Force Communications Agency/Combat Information Transport System.

Air Force Communications Agency. (2007b, 5 October). Combat Information Transport System Block 30 Spiral 2: System Requirements Document (Draft). Scott AFB, Belleville, IL: Air Force Communications Agency/Electronic Communications Network. Air Force Communications Agency/Combat Information Transport System.

Air Force Space Command. (2009, November). The United States Air Force blueprint for cyberspace. Peterson Air Force Base, CO: AFSPC.

Alberts, D., S., & Hayes, R. E. (2003). *Power to the Edge: Command…Control…in the Information Age.* Washington, DC: CCRP, 2003.

Alliger, G. M., Beard, R., Bennett, W. Jr., Colegrove, C. M., & Garrity, M. (2007). Understanding Mission Essential Competencies as a Work Analysis Method (AFRL-HE-AZ-TR-2007-0034). Mesa, AZ: Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Readiness Research Division.

Anderson, J. R. (1983). *The architecture of cognition*. Cambridge, MA: Harvard University Press.

Anderson, J. R., Boyle, C. F., Farrell, R., & Reiser, B. (1984). *Cognitive principles in the design of computer tutors* (ADA144825). Paper presented at the *6th Annual Conference of the Cognitive Science Society*, Boulder, CO.

Anderson, J. R., Corbett, A. T., Koedinger, K. R., & Pelletier, R. (1995). Cognitive tutors: Lessons learned. The *Journal of the Learning Sciences, 4*(2), 167-207.

Andrews, D.H., Carroll, L.A., Bell, H.H. (1996). The Future of Selective Fidelity in Training Devices (DTIC ADA316902). Wright-Patterson Air Force Base, OH: Armstrong Lab Human Resources Directorate.

Aptima, Inc. (2008, July 15). Development of NOD Mission Essential Competencies (MECs)SM (Technical Report). Woburn, MA: Author.

Aptima, Inc. (2009, September 8). Development of AFCERT Mission Essential Competencies (MECs)SM (Technical Report). Woburn, MA: Author.

Aptima, Inc. (2010, January 18). Development of INOSC-East Mission Essential Competencies (MECs)SM (Technical Report). Woburn, MA: Author.

Ashley, K. D., Chi, M., Pinkus, R., & Moore, J. D. (2004). *Modeling learning to reason with cases in engineering ethics: A test domain for intelligent assistance* (NSF Proposal No. NSF-LIS 9720341).

Beck, J., Stern, M., & Haugsjaa, E. (1996). Applications of AI in education. *ACM Crossroads, 3*, 11-15.

Bloom, B. S. (1984). The 2 sigma problem: The search for methods of group instruction as effective as one-to-one tutoring. *Educational Researcher, 13*(6), 4-16.

Bolstad, C. A., & Endsley, M. R. (2003). Measuring shared and team situation awareness in the Army's future objective force. In *Proceedings of the Human Factors and Ergonomics Society 47th Annual Meeting- 2003* (pp. 369-373). Santa Monica, CA: Human Factors and Ergonomics Society.

Bransford, J. D., Brown, A. L., & Cocking R. R. (Eds.). (2000). *How people learn: Brain, mind, experience, and school* (Expanded Edition). Washington, D.C.: National Academy Press.

Brown, J. S., Collins, A., & Duguid, P. (1989). Situated cognition and the culture of learning. *Educational Researcher, 18*, 32-42.

Brueckner, S., Guaspari, D., Adelstein, F., & Weeks, J. (2008). Automated computer forensics training in a virtualized environment. *Digital Investigation, 5,* S105-S111.

Buchan, G. C. (1999). Strategic appraisal: The changing role of information in warfare. *Rand Strategic Appraisal Series,* 283-323.

Bürki-Cohen, J., Soja, N. N., & Longridge, T. (1998). Simulator platform motion—The need revisited. *The International Journal of Aviation Psychology*, *8*(3) 293-317.

Bürki-Cohen, J., Sparko, A.L., & Go, T.H. (2007). *Training Value of a Fixed-Base Flight Simulator with a Dynamic Seat*. AIAA Modeling and Simulation Technologies Conference and Exhibit 20 - 23 August 2007, Hilton Head, SC (AIAA 2007-6564).

Cannon-Bowers, J. A., & Salas, E. (1998). Individual and team decision making under stress: theoretical underpinnings. In J. Cannon-Bowers, & E. Salas (Eds.), *Making decisions under stress: Implications for individual and team training* (pp. 17-38). Washington, DC: American Psychological Association.

Cannon-Bowers, J. A., & Salas, E. (2001). Reflections on shared cognition. *Journal of Organizat*ional *Behavior, 22*, 195-202.

Cannon-Bowers, J. A., Salas, E., & Converse, S. (1993). Shared mental models in expert team decision making. In N. J. Castellan (Ed.), *Individual and Group Decision Making* (pp. 221-246). Hillsdale, NJ: Lawrence Erlbaum.

Cannon-Bowers, J., & Bowers, C. (2009). Training Support Technologies: Section Perspective. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 2: VE Components and Training Technologies* (pp. 263-269). Westport, CT: Praeger Security International.

Carayon, P. (2006). Human factors of complex sociotechnical systems. *Applied Ergonomics, 37,* 525-535.

Center for Innovative Learning Technologies (CILT). (2004). *Design principles for educational software.* Retrieved from http://www.design-principles.org.

Cherns, A. (1976). The principles of sociotechnical design. *Human Relations, 29,* 783-792.

Chung, W.W.Y. (2000). A review of approaches to determine the effectiveness of ground-based flight simulations. AIAA Modeling and Simulation Technologies Conference, 14-17 August 2000, Denver, CO (AIAA-2000-4298).

Cohn, J., Schmorrow, D., Lyons, D., Templeman, J., & Muller, P. (2003). Virtual Technologies and Environments for Expeditionary Warfare Training. Paper presented at the RTO HFM Symposium on Advanced Technologies for Military Training, Genoa, Italy, 13 – 15 October 2003.

Colegrove, C. (2004). Competency-based training. Presented at the Combat Air Forces Distributed Mission Operations Users' Conference.

Colegrove, C. M., & Alliger, G. M. (2002). Mission Essential Competencies: Defining combat mission readiness in a novel way. Paper presented at the NATO RTO Studies, Analysis and Simulation Panel (SAS) Symposium. Brussels, Belgium.

Colegrove, C. M., & Bennett, W. Jr. (2006). Competency-based Training: Adapting to Warfighter Needs (AFRL-HE-AZ-TR-2006-0014). Mesa, AZ: Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Readiness Research Division.

Collins, A., Brown, J. S., & Newman, S. E. (1989). Cognitive apprenticeship: Teaching the crafts of reading, writing, and mathematics. In L. B. Resnick (Ed.), *Knowing, learning and instruction: Essays in honor of Robert Glaser* (pp. 453-494). Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Collyer, S. C., & Malecki, G. S. (1998). Tactical decision making under stress: History and overview. In J. Cannon-Bowers, & E. Salas (Eds.), *Making decisions under stress: Implications for individual and team training* (pp. 3-15). Washington, DC: American Psychological Association.

Cooke, N. J. (1999). Knowledge elicitation. In F.T. Durso (Ed.), *Handbook of Applied Cognition* (pp. 479-509). Chichester, England: John Wiley & Sons.

Cooke, N. J., & Gorman, J. C. (2006). Assessment of team cognition. In P. Karwowski (Ed.), *International Encyclopedia of Ergonomics and Human Factors* (2nd ed., pp. 270-275). London, England: Taylor & Francis.

Cooke, N. J., Gorman, J. C., & Rowe, L. J. (2009). An ecological perspective on team cognition. In E. Salas, G. F. Goodwin, & C. S. Burke (Eds.), *Team Effectiveness in Complex Organizations: Cross-Disciplinary Perspectives and Approaches* (pp. 157-182). New York, NY: Routledge.

Cooke, N. J., Gorman, J. C., & Winner, J. L. (2007). Team cognition. In F. T. Durso (Ed.), *Handbook of Applied Cognition* (2nd ed., pp. 239-268). Chichester, England: John Wiley & Sons.

Cooke, N. J., Kiekel, P. A., & Helm, E. E. (2001). Measuring team knowledge during skill acquisition of a complex task. *International Journal of Cognitive Ergonomics, 5*(3), 297-315.

Cooke, N. J., Salas, E., Cannon-Bowers, J. A., & Stout, R. J. (2000). Measuring team knowledge. *Human Factors, 42*(1), 151-173.

Cooke, N. J., Stout, R. J., & Salas, E. (2001). A knowledge elicitation approach to the measurement of team situation awareness. In M. McNeese, M. Endsley, & E. Salas (Eds.), *New Trends in Cooperative Activities: System Dynamics in Complex Settings* (pp. 114-139). Santa Monica, CA: Human Factors.

Corbett, A. T., Koedinger, K. R., & Hadley, W. H. (2001). Cognitive tutors: From the research classroom to all classrooms. In P. S. Goodman (Ed.), *Technology enhanced learning: Opportunities for change.* Mahwah, NJ: Lawrence Erlbaum Associates.

Costello, A. M., Strater, L., Bolstad, C. A., Cuevas, H. M., & Endsley, M. R. (2006). *Communication and situation awareness in ad hoc teams*. Marietta, GA: SA Technologies.

D'Amico, A., & Larkin, M. (2001). Methods of visualizing temporal patterns in and mission impact of computer security breaches. *Proceedings of the DARPA Information Survivability Conference and Exposition, 1*, 343-351.

Dammon, C. T., & Lane, D. M. (1993). Transfer of training in a fault diagnosis task. Proceedings of the Human Factors and Ergonomics Society 37th Annual Meeting, 1272-1276.

de Vries, P., Midden, C., & Bouwhuis, D. (2003). The effects of error on system trust, self-confidence, and the allocation of control in route planning. *International Journal of Human-Computer Studies, 58,* 719-735.

Dubois, D., & Rothwell, W. (2004). Competency-based or a traditional approach to training? A new look at ISD models and an answer to the question, What's the best approach? *T+D: better performance through workplace learning*, *58*(4). Alexandria, VA: American Society for Training and Development. Retrieved from (http://findarticles.com/p/articles/mi_m0MNT/is_4_58/ai_n6121342/).

Duncan, K. D. (1987). Fault diagnosis training for advanced continuous process installations. In J. Rasmusse, K. Duncan, and J. Leplat (Eds.) *New Technology and Human Error.* New York, NY: John Wiley & Sons Ltd.

Dzindolet, M. T., Peterson, S. A., Pomranky, R. A., Pierce, L. G., & Beck, H. P. (2003). The role of trust in automation reliance. *International Journal of Human-Computer Studies, 58,* 697-718.

Ehrlich, J. A., Knerr, B. W., Lampton, D. R., & McDonald, D. P. (1997). *Team situational awareness training in virtual environments: Potential capabilities and research issues* (ADA337606). Alexandria, VA: U. S. Army Research Institute for the Behavioral and Social Sciences.

Espinosa, J. A., Kraut, R. E., Slaughter, S. A., Lerch, J. F., Herbsleb, J. D., & Mockus, A. (2002). Shared mental models, familiarity, and coordination: A multi-method study of distributed software teams. In *23rd International Conference on Information Systems, December 2002, Barcelona, Spain Proceedings*. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1131&context=icis2002.

Flach, J. M. (1995). Situation awareness: Proceed with caution. *Human Factors, 37*(1), 149-157.

Fowlkes, J., Dwyer, D. J., Oser, R. L., & Salas, E. (1998). Event-based approach to training. *The International Journal of Aviation Psychology, 8*(3), 209-221.

Freeman, J., Stacy, W., & Olivares, O. (2009). Measurement and assessment for training in virtual environments. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI handbook of virtual environments for training and education: Developments for the military and beyond. Volume 2: VE Components and Training Technologies* (pp. 236-250). Westport, CT: Praeger Security International.

Gorman, J. C., Cooke, N. J., & Winner, J. L. (2006). Measuring team situation awareness in decentralized Command and Control systems. *Ergonomics, 49,* 1312-1325.

Gorman, J. C., Cooke, N. J., Pederson, H. K., Connor, O. O., & DeJoode, J. A. (2005). Coordinated awareness of situation by teams (CAST): Measuring team situation awareness of a communication glitch. In *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting* (pp. 274-277). Santa Monica, CA: Human Factors and Ergonomics Society.

Gualtieri, J., Burns, J., Phipps, D., Reeves, D., & Pierce, L. (1998). Assessing team knowledge structures: Findings from the field. In *Proceedings of the Human Factors and Ergonomics Society 42nd Annual Meeting- 1998* (pp. 1417-1421). Santa Monica, CA: Human Factors and Ergonomics Society.

Guzdial, M. (1994). Software-realized scaffolding to facilitate programming for science learning. *Interactive Learning Environments, 4*, 1-44.

Ham, D., & Yoon, W. C. (2007). The training effects of principle knowledge on fault diagnosis performance. *Human Factors and Ergonomics in Manufacturing, 17,* 263-282.

Hays, R. T. (2006). *The science of learning: A systems theory approach.* Boca Raton, FL: Brown Walker Press.

Hazeur, E. L. Jr. (2010, March 9). *09-11 February 2010 AOC FTU Syllabus Review Conference Meeting Minutes*. Hurlburt Field, FL: Department of the Air Force.

Hershey, T. (2008). Realistic Distributed Network Training Environment for Networked Operations [Cyber ATC Data Call Template]. Unpublished. Air Force Cyber Command: Applied Technology Counsel.

Hideshima, Y., & Koike, H. (2006, February). STARMINE: A visualization system for cyber attacks. In K. Misue, K. Sugiyama, & J. Tanaka (Eds.) *Proceedings of the 2006 Asia-Pacific Symposium on Information Visualization,* Vol 60, Tokyo, Japan.

Holsopple, J., Yang, S. J. , Kuhl, M., Hall, D., Nagi, R., Shapiro, S., Sudit, M., Panulla, B., Kandefer, M., Seyed, P., Ying, Z., Gosavi, A., Costantini, K., &, Tauer, G. (2009). *National Center for Multisource Information Fusion* (ADA496940). Buffalo, NY: Calspan University of Buffalo Research Center.

Honebein, P. C. (1996). Seven goals for the design of constructivist learning environments. In B. Wilson (Ed.), *Constructivist learning environments: Case studies in instructional design*. Englewood Cliffs, NJ: Educational Technology Publications, Inc.

Jabbour, K. (2009). The science and technology of cyber operations. *High Frontier: The Journal for Space & Missile Professionals, 5,* 11-15.

Johnson, L., Rickel, J., & Lester, J. (2000). Animated pedagogical agents: face-to-face interaction in interactive learning environments. *The International Journal of Artificial Intelligence in Education, 11,* 47-78.

Joint Chiefs of Staff. (2009, June 24) Chairman of the Joint Chiefs of Staff manual: Information assurance (IA) and computer network defense (CND) Vol I (Incident Handling Program) (CJCSM 6510.01A). Washington, DC: Author.

Kamradt, H., & MacDonald, D. (1998). The implications of network-centric warfare for United States and multinational military operations (Decision Support Department Occasional Paper 98-1). Newport, RI: US Naval War College, Center For Naval Warfare Studies.

Katz, S. (2010, April 15). *Cyber modeling & simulation (M&S) study*. Retrieved from https://halfway.peterson.af.mil/SARP/Studies/Default.aspx?Page=view&StudyID=5015.

Kean, Elizabeth S., personal communication, April 12, 2010, Air Force Research Laboratory, Information Directorate (AFRL/RISA), 525 Brooks Rd, Rome, NY 13441-4505, (315)330-2601, Elizabeth.Kean@rl.af.mil.

Kirkpatrick, D. (1976). Evaluation of training. In R. L. Craig (Ed.), *Training and development handbook: A guide to human resources development* (pp. 18.1 – 12.27). New York, NY: McGraw-Hill.

Kirkpatrick, D. (1996). Revisiting Kirkpatrick's four-level model. *Training and development, 1,* 54-57.

Klein, G. (2009, March). COVE: *A macrocognitive view*. Paper presented at the Cyberspace Operations Virtual Environment (COVE) Workshop, Mesa, Arizona.

Klimoski, R., & Mohammed, S. (1994). Team mental model: Construct or metaphor? *Journal of Management, 20*(2), 403-437.

Kocka, M., & D'Amico, A. (2004). *Data presentation best practices: A resource for developing cyber situational awareness displays-Final Report* (Report CSA-VIZ-1). Fort George G. Meade, MD: Department of Defense/Air Force Research Laboratory.

Krokos, K. J., Baker, D. P., Alonso, A., & Day, R. (2009). Assessing team processes in complex environments: Challenges in transitioning research to practice. In E. Salas, G. F. Goodwin, & C. S. Burke (Eds.), *Team Effectiveness in Complex Organizations: Cross-Disciplinary Perspectives and Approaches* (pp. 383-408). New York, NY: Routledge.

Kumaraguru, P., & Sheng, S. (2008). Lessons from a real world evaluation of anti-phishing training. In *Proceedings of the eCrime Researchers Summit, 2008*. Atlanta, GA: APWG.

Lampton, D., Martin, G, Meliza, L, & Goldberg, S. (2009). After Action Review in Simulation Based Training. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 2: VE Components and Training Technologies* (pp. 297-310). Westport, CT: Praeger Security International.

Lane, H. C., & Johnson, L. (2009). Intelligent tutoring and pedagogical experience manipulation in virtual learning environments. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 1: Learning Requirements, and Metrics* (pp. 393-406). Westport, CT: Praeger Security International.

Lee, J. D., & Moray, N. (1994). Trust, self-confidence, and operators' adaptation to automation. *International Journal of Human-Computer Studies, 40*, 153-184.

Lee, J. D., & See, K. A. (2004). Trust in automation. *Human Factors, 46,* 50-80.

Lengler, R., & Eppler, M. J. (2007). Towards a periodic table of visualization methods for management. *Proceedings of Graphics and Visualization in Engineering.* Clearwater, FL: ACTA Press.

Lester, J., Converse, S., Kahler, S., Barlow, T., Stone, B., & Bhogl, R. (1997). The persona effect: Affective impact of animated pedagogical agents. In *Proceedings of CHI 1997* (pp. 359-366). Atlanta, GA: ACM

Lester, J., Converse, S., Stone, B., Kahler, S., & Barlow, T. (1997). Animated pedagogical agents and problem-solving effectiveness: a large-scale empirical evaluation. In B. du Boulay & R Mizoguchi (Eds.), *Artificial intelligence in education: Knowledge and media in learning systems* (pp. 23-30). Fairfax, VA: IOS Press.

Levine, A. (2009, April 7). *Official: Millions spent defending Pentagon computers from attack*. Retrieved from http://www.cnn.com/2009/POLITICS/04/07/military.computers/index.html.

Levis, A. H. (2009, March). *Training airmen to operate in a contested cyber environment*. Paper presented at the Cyberspace Operations Virtual Environment (COVE) Workshop, Mesa, Arizona.

Linn, M. C., Davis, E. A., & Eylon, B. S. (2004). The scaffolded knowledge integration framework for instruction. In M. C. Linn, E. A. Davis & P. Bell (Eds.), *Internet environments for science education* (pp. 47-72). Mahwah, NJ: Lawrence Erlbaum Associates, Inc.

Lynch, C. F., Ashley, K. D., Aleven, V., & Pinkwart, N. (2006). Defining "ill-defined domains": A literature survey*. In Proceedings of the 8th International Conference of Intelligent Tutoring Systems,* Jhongli, Taiwan.

Ma, K-L. (2004). Visualization for security. *Computer Graphics, 38,* 4-6.

Macmillan, N. A., & Creelman, C. D. (1991). *Detection theory: A user's guide*. Cambridge, MA: Cambridge University Press.

Maguire, M. (2001). Methods to support human-centered design. *International Journal Human-Computer Studies, 55*, 587-634.

Masalonis, A. J., (2003). Effects of training operators on situation-specific automation reliability. *2003 IEEE International Conference on Systems, Man, and Cybernetics,* 1595-1599.

May, Thomas, personal communication, March 17, 2010 USAF AFSPC AFNIC/ESFF, 203 W. Losey Street, Scott Air Force Base, IL 62225, (618) 229-6277, thomas.may@us.af.mil

McCauley, M. E. (2006). *Do army helicopter training simulators need motion bases?* (Technical Report No. 1176). Arlington, VA: United States Army Research Institute for the Behavioral and Social Sciences.

McGuirl, J. M., & Sarter, N. B. (2006). Supporting trust calibration and the effective use of decision aids by presenting dynamic system confidence information. *Human Factors, 48,* 656-665.

Menaker, E., Coleman, S., Collins, J., & Murawski, M. (2006). Harnessing experiential learning theory to achieve warfighting excellence. *Proceedings of Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC*). Orlando, FL: National Security Industrial Association.

Merritt, S. M., & Ilgen, D. R. (2008). Not all trust is created equal: dispositional and history-based trust in human-automation interactions. *Human Factors, 50,* 194-210.

Meserve, J. (2009, April 9). *Hackers reportedly have embedded code in power grid*. CNN.com. Retrieved from http://www.cnn.com/2009/TECH/04/08/grid.threat/index.html.

Mesic, R., Hura, M., Libicki, M. C., Packard, A. M., & Scott, L. M. (2010). *Air Force Cyber Command (Provisional) Decision Support*. Santa Monica, CA: Rand Corporation.

Milham, L., Carroll, M. B., Stanney, K., & Becker, W. (2009). Training Systems Requirements Analysis. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 2: VE Components and Training Technologies* (pp. 165-192). Westport, CT: Praeger Security International.

Miller, J. (2009). *'Quick Look' interim report: Trust in cyberdomains research roadmap recommendations. Preliminary findings from working meeting 14 -16 July 2009* Pensacola Beach, FL. Dayton, OH: SRA International.

Minsky, M. (1995). Steps to artificial intelligence. In Luger, G. F. (Ed.), *Computation and Intelligence, Collected Readings* (pp. 47-90). Menlo Park, CA: MIT Press.

Mohammed, S., & Dumville, B. C. (2001). Team mental models in a team knowledge framework: Expanding theory and measurement across disciplinary boundaries. *Journal of Organizational Behavior, 22*, 89-106.

Molenda, M. (2003). In search of the elusive ADDIE model. *Performance improvement, 42*(5), 34.

Moreno, R., Mayer, R., & Lester, J. (2000). Life-like pedagogical agents in constructivist multimedia environments: Cognitive consequences of their interaction. In *Proceedings of the World Conference on Educational Multimedia, Hypermedia, and Telecommunications (ED-MEDIA).* Montreal, Canada (pp. 741-746). Charlottesville, VA: Association for the Advancement of Computing in Education.

Morris, N. M., & Rouse, W. B. (1985). Review and evaluation of empirical research in troubleshooting. *Human Factors, 27,* 503-530.

National Academy of Engineering. (2008). *Grand Challenges for Engineering*. Retrieved from www.engineeringcchallenges.org.

Nielsen, J. (1994). Heuristic evaluation. In J. Nielsen & R. L. Mack (Eds.), *Usability Inspection Methods*, New York, NY: John Wiley & Sons

Norman, D. A. (1986). Cognitive engineering. In D. A. Norman & S. W. Draper (Eds.), *User centered system design*. Mahwah, NJ: Lawrence Erlbaum Associates.

O'Connor, F. (2009, March 12). Political Cyberattacks to Militarize the Web. *PCWorld.com.* Retrieved from http://www.pcworld.com/businesscenter/article/161142/political_cyberattacks_to_militarize_the_web.html

Ockerman, J. J., Case, F. T., Koterba, N. T., Huguenin, B. A., & Garcia, O. A. (2008). Automatic collection of process data to support Air Force dynamic targeting instructors. In *Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting- 2008* (pp. 595-599). Santa Monica, CA: Human Factors and Ergonomics Society.

Okolica, J., McDonald, T., Peterson, G., Mills, R., & Haas, M. (2009). *Developing systems for cyber situational awareness.* In Proceedings of the 2nd Cyberspace Research Workshop, Shreveport, LA.

Papert, S. (1993). *The children's machine: Rethinking school in the age of the computer*. New York, NY: Basic Books.

Parasuraman, R., & Riley, V. (1997). Humans and automation: use, misuse, disuse, abuse. *Human Factors, 39,* 230-253.

Parasuraman, R., Masalonis, A. J.& Hancock, P. A. (2000). Fuzzy signal detection theory: Basic postulates and formulas for analyzing human and machine performance. *Human Factors, 42*, 636 – 659.

Pasmore, W. A. (1988). *Designing Effective Organizations: The Sociotechnical Systems Perspective*. New York, NY: John Wiley & Songs.

Patrick, J., Grainger, L., Gregov, A., Halliday, P., Handley, J., James, N., & O'Reilly, S. (1999). Training to break the barriers of habit in reasoning about unusual faults. *Journal of Experimental Psychology: Applied, 5,* 314-335.

Pea, R. D. (2004). The social and technological dimensions of scaffolding and related theoretical concepts for learning, education, and human activity. *The Journal of the Learning Sciences, 13*(3), 423-451.

Piaget, J. (1954). *The construction of reality in the child*. New York, NY: Basic Books.

Portrey, A. M., Keck, L. B., & Schreiber, B. T. (2006). *Challenges in developing a performance measurement system for the global virtual environment* (AFRL-HE-AZ-TR-2006-0022). Mesa, AZ: Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Readiness Research Division.

Proctor, R. W., & Van Zandt, T. (1994). *Human Factors in Simple and Complex Systems.* Needham Heights, MA: Allyn and Bacon.

Prost, J. H., Schreiber, B. T., & Bennett, W. Jr. (2008). Incidental changes to training capabilities due to technological improvements (AIAA 2008-6681/ADA494803**)**. American Institute of Aeronautics and Astronautics (AIAA) Modeling and Simulation Technologies Conference and Exhibit. 18 - 21 August 2008, Honolulu, HI.

Prost, J. H., Schreiber, B. T., & Bennett, W. Jr., (2007). Identification and evaluation of simulator system deficiencies. In *2007 Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) Proceedings*. Orlando, FL: National Security Industrial Association.

Prost, J. H., Schreiber, B. T., Bennett, W. Jr., & Kleinlein, K. B. (2008). *Providing effective and efficient training: A model for comparing simulator improvements* (08F-SIW-007). Paper presented at the 2008 Fall Simulation Interoperability Workshop. Orlando, FL: SISO.

Quintana, C., Krajcik, J., & Soloway, E. (2001). Exploring a description and methodology for learner-centered design. In W. Heineke & L. Blasi (Eds.), *Methods of evaluating educational technology*, Vol. 1. Greenwich, CT: Information Age Publishing.

Quintana, C., Krajcik, J., & Soloway, E. (2003). Issues and approaches for developing learner-centered technology. *Advances in Computers, 57*, 271-321.

Quintana, C., Reiser, B. J., Davis, E. A., Krajcik, J, Fretz, E., Golan Duncan, R., Kyza, E., Edelson, D., & Soloway, E. (2004). A scaffolding design framework for software to support science inquiry. *The Journal of the Learning Sciences, 13*(3), 337-386.

Reason, J. (1990). *Human Error.* Cambridge University Press: New York.

Reising, D. V. (1993). Diagnosing multiple simultaneous faults. *Proceedings of the 37th Annual Meeting of the Human Factors and Ergonomics Society* (pp. 524-528).

Rickel, J., & Johnson, W. L. (1997). Intelligent tutoring in virtual reality: A preliminary report. In *Proceedings of the Eighth World Conference on Artificial Intelligence in Education* (pp. 294-301). Amsterdam, Netherlands: IOS Press.

Riley, J. M., Endsley, M. R., Bolstad, C. A., & Cuevas, H. M. (2006). Collaborative planning and situation awareness in Army Command and Control. *Ergonomics, 49*(12-13), 1139-1153.

Riley, J., Kaber, D, Sheik-Nainar, M., & Endsley, M. (2009). Enhancing Situation Awareness Training in Virtual Reality Through Measurement and Feedback. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 2: VE Components and Training Technologies* (pp. 326-347). Westport, CT: Praeger Security International.

Robertson, G., Czerwinski, M., Fisher, D., & Lee, B. (2009). Selected human factors issues in information visualization. *Reviews of Human Factors Issues in Information Visualization, 5,* 41-81.

Rossey, L. M., Rabek, J. C., Cunningham, R. K., Fried, D. J., Lippman, R. P., & Zissmann (2001, October). *LARIAT: Lincoln adaptive real-time information assurance test-bed.* Paper presented at the International Symposium on Recent Advances in Intrusion Detection (RAID), Davis, CA.

Roth, E., Stilson, M. , Scott, R., Whitaker, R., Kazmierczak, T., Thomas-Myers, G., & Wampler, J. (2006). *Work-Centered Design and Evaluation of a C2 Visualization Aid* (AFRL-HE-WP-TP-2006-0078). Dayton, OH: Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Interface Division, Cognitive Systems Branch, Wright-Patterson AFB.

Rovira, E., McGarry, K.,& Parasuraman, R. (2007). Effects of imperfect automation on decision making in simulated command and control task. *Human Factors, 49,* 76-87.

Rowe, L. J., Gehr, S. E., Cooke, N. J., & Bennett, W., Jr. (2007). Assessing Distributed Mission Operations using the air superiority knowledge assessment system. In P*roceedings of the Human Factors and Ergonomics Society's Annual Meeting* (pp. 1569-1572). Santa Monica, CA: Human Factors and Ergonomics Society.

Salas, E., Prince, C., Baker, D. P., & Shrestha, L. (1995). Situation awareness in team performance: Implications for measurement and training. *Human Factors, 37*(1), 123-136.

Salerno, J J., & Tadda, G. P. (2009). *Ranking Activities Based on Their Impact and Threat* (A374705). Rome, NY: Air Force Research Laboratory, Information Directorate.

Salerno, J. J. (2008). Measuring Situation Assessment Performance through the Activities of Interest Score. In *Proceedings of the 11th International Conference on Information Fusion*, Cologne GE, June 30 – July 3, 2008 (pp. 326-333).

Salomon, G., Perkins, D. N., & Globerson, T. (1991). Partners in cognition: Extending human intelligence with intelligent technologies. *Educational Researcher*, *20*(3), 2-9.

Sanders, M. S., & McCormick, E. J. (1993). *Human factors in engineering and design* (7th ed.). New York, NY: McGraw-Hill.

Schaafstal, A., Schraagen, J. M., & van Berlo, M. (2000). Cognitive task analysis and innovation of training: the case of structured troubleshooting. *Human Factors, 42,* 75-86.

Schreiber, B. T., DiSalvo, P, Stock, W. A., & Bennett, W. Jr. (2006). *Distributed Mission Operations within-simulator training effectiveness baseline study: Using the Pathfinder methodology to assess pilot knowledge structure changes* (AFRL-HE-AZ-TR-2006-0015-Vol V). Mesa, AZ: Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Readiness Research Division.

Schreiber, B. T., Watz, E., Bennett, W. Jr., & Portrey, A. M. (2003). *Development of a Distributed Mission Training automated performance tracking system*. Paper presented at 2003 Conference on Behavior Representation in Modeling and Simulation, Scottsdale, AZ. Retrieved from, http://www.sisostds.org/index.php?tg=fileman&idx=get&id=2&gr=Y&path=CGF-BRIMS%2F12th+CGF-BR%2F12th+CGF-BR+Papers+and+Presentations&file=03-BRIMS-062.pdf.

Schvaneveldt, R., Tucker, R., Castillo, A., & Bennett, W., Jr. (2001). Knowledge acquisition in Distributed Mission Training. In *2001 Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC).* Orlando, FL: National Training Systems Association.

See, J. E., Riegler, J. T., Fitzhugh, E., & Kuperman, G. G. (1996). *Unaided Target Acquisition Performance with First Generation Forward-Looking Infrared Imagery: A Signal Detection Theory Analysis* (Report No. AL/CF-TR-1996-0094). Wright-Patterson Air Force Base, OH: Armstrong Laboratory.

See, J. E., Warm, J. S., Dember, W. N., & Howe, S. R. (1997). Vigilance and Signal Detection Theory: An Empirical Evaluation of Five Measures of Response Bias. *Human Factors, 39*(1), 14-29.

Seong, Y., & Bisantz, A. M. (2008). The impact of cognitive feedback on judgment performance and trust with decision aids. *International Journal of Industrial Ergonomics, 38,* 608-625.

Shadrick, S., & Lussier, J. (2009). Knowledge Elicitation: The FLEX Approach. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 1: Learning Requirements, and Metrics* (pp. 363-377)*.* Westport, CT: Praeger Security International.

Shane, S., & Drew, C. (2009, December 17). Officials say Iraq fighters intercepted drone video. *New York Times.* Retrieved from *http://www.nytimes.com/2009/12/18/world/middleeast/18drones.html?_r=2*.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of CHI 2010,* April 10-15, 2010. Atlanta, GA: ACM.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. *In Proceedings of the 3rd Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, July 18-20, 2007) (pp. 88-99). ACM, New York, NY..

Singer, M., & Howey, A. (2009). Enhancing virtual environments to support training. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 1: Learning Requirements, and Metrics* (pp. 407-421). Westport, CT: Praeger Security International.

Skinner, B. F. (1958). Teaching machines: From the experimental study of learning come devices which arrange optimal conditions for self-instruction. *Science, 128*(3330), 969-77.

Soloway, E., Guzdial, M., & Hay, K. E. (1994). Learner-centered design: The challenge for HCI in the 21st century. *Interactions, 1*, 36-48.

Stanton , N. A., Stewart, R., Harris, D., Houghton, R.J., Baber, C., McMaster, R., Salmon, P., Hoyle. G., Walker, G., Young. M. S., Linsell, M., Dymott, R.& Green, D. (2005). *Distributed situation awareness in Command and Control: A case study in the energy distribution domain.* Paper presented at the HCI International 2005- 11th International Conference on Human-Computer Interaction, Las Vegas, NV. Hillsdale, NJ: Lawrence Erlbaum.

Stock, W. A., Schreiber, B. T., Denning, T., & Cain, D (2006). *AOC Embedded performance measurement and assessment* (AFRL-HE-AZ-TR-2006-0025). Mesa, AZ: Air Force Research Laboratory, Human Effectiveness Directorate, Warfighter Readiness Research Division.

Stout, R, Bowers, C., & Nicholson, D. (2009). Guidelines for Using Simulations to Train Higher Level Cognitive and Teamwork Skills. In D. Schmorrow, J. Cohn & D. Nicholson (Eds.), *The PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Volume 2: VE Components and Training Technologies* (pp. 270-296). Westport, CT: Praeger Security International.

Swets, J. A., Tanner, W. P., Jr., & Birdcall, T. G. (1961). Decision Processes in perception. *Psychological Review, 68*, 301-340.

Tadda, G. P. (2008). Measuring the Performance of Cyber Situation Awareness Systems. In *Proceedings of the 11th International Conference on Information Fusion*, Cologne GE, June 30 – July 3, 2008 (pp. 334-342).

Thomas, J. J., & Cook, K. A. (2005). *Illuminating the Path: The Research and Development Agenda for Visual Analytics*. National Visualization and Analytics Center.

Trefz, J. L. Jr. (2008). [Untitled]. PowerPoint presented at the USSTRATCOM Science & Technology Conference. Newport, RI: Network Operations/Network Warfare Division.

Tsang, P. S., Vidulich, M. A. (2002). *Principles and practice of aviation psychology.* Mahwah, NJ: Lawrence Erlbaum Associates.

Uhlarik, J., & Comerford, D. A. (2002). *A review of situation awareness literature relevant to pilot surveillance functions* (Report No. DOT/FAA/AM-02/3). Washington, DC: Government Printing Office.

United States Air Force Scientific Advisory Board. (2007a). *Report on Implications of Cyber Warfare Volume 1: Executive summary and annotated brief* (SAB-TR-07-02). Washington, DC: Department of the Air Force, HQ USAF/SB.

United States Air Force Scientific Advisory Board. (2007b). *Report on Implications of Cyber Warfare Volume 2: Final Report* (SAB-TR-07-02). Washington, DC: Department of the Air Force, HQ USAF/SB.

United States Air Force Scientific Advisory Board. (2008). *Report on Defending and Operating in a Contested Cyber Domain: Executive Summary and Annotated Brief* (SAB-TR-08-01). Andrews AFB, MD: Department of the Air Force, HQ USAF/SB.

United States. (31 November 2008). *Cyberspace Operations*, Air Force doctrine document 2-11. Washington, D.C.: U.S. Air Force.

VanLehn, K. (1989). Problem solving and cognitive skill acquisition. In M. Posner (Ed.), *Foundations of cognitive science* (pp. 527-580). Cambridge, MA: MIT Press.

Vice Chairman of the Joint Chiefs of Staff. (2008, September 29). Action memo: Definition of cyberspace operations. Washington, DC: Department of Defense.

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Cambridge, MA: Harvard University Press.

Wabiszewski, M. G., Andel, T. R., Mullins, B. E., & Thomas, R. W. (2009). Enhancing realistic hands-on network training in a virtual environment. *Proceedings of the 2009 Spring Simulation Multiconference,* San Diego, CA.

Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A review of sociotechnical systems theory: a classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science, 9,* 479-499.

Wampler, J., Whitaker, R., Roth, R., Scott, R., Stilson, M., & Thomas-Meyers, G. (2005). Cognitive work aids for C2 planning: Actionable information to support operational decision making. In *Proceedings of the 10th International Command and Control Research and Technology Symposium. The Future of C2.* Washington, DC: DOD: Office of the Assistant Secretary of Defense.

Wang, X. (2007). The theoretical framework of cognitive informatics. *International Journal of Cognitive Informatics and Natural Intelligence, 1*, 1-27.

Ware, C. (2004). *Foundation for a science of data visualization. In Information Visualization: Perception for design.* San Francisco, CA: Morgan Kaufman.

Weeks, J. (2009). *General discussion*. Cyberspace Operations Virtual Environment (COVE) [Workshop], March 12-13, 2009. Air Force Research Laboratory, Mesa, AZ.

Wilson, B. (1996). What is a constructivist learning environment? In B. Wilson (Ed.), *Constructivist learning environments: Case studies in instructional design*. Englewood Cliffs, NJ: Educational Technology Publications, Inc.

Wood, D., Bruner, J., & Ross, G. (1976). The role of tutoring in problem solving. *Journal of Child Psychology and Psychiatry and Allied Disciplines, 17*, 89-100.

Wray, R., Lane, H. C., Stensrud, B., Core, M. Hamel, L., & Forbell, E. (2009). *Pedagogical Experience Manipulation for Cultural Learning*. S. D. Craig & D. Dicheva (Eds.), AIED 2009: 14th International Conference on Artificial Intelligence in Education Workshops Proceedings (pp. 35-44). Brighton, UK: AIED.

Yao, Y. Y. (2004). Concept formation and learning: A cognitive informatics perspective. International Conference on Cognitive Informatics (ICCI'04), August 2004, (pp. 42-51).

Yoon, W. C., & Hammer, J. M. (1988). Aiding the operator during novel fault diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics, 18,* 142-148.

Zacharias, G. (2009, March). *Human systems engineering design considerations for COVE*. Paper presented at the Cyberspace Operations Virtual Environment (COVE) Workshop, Mesa, AZ.

8 Appendix A
Team Members and Contributors

Air Force Research Laboratory

Dr Joseph L. Weeks, Principal Investigator, Cyber Distributed Mission Operations Research

Lumir Research Institute, Inc.

Jennifer Winner, Research Scientist, Task Order Lead

Lisa Holt, Senior Research Scientist

Jasmine Duran, Research Scientist

William Stock, Senior Research Scientist

Eric Watz, Senior Software Engineer

PatchPlus Consulting, Inc.

Kristin Steinke, Senior Intelligence Consultant

Kim Noble, Senior Intelligence Consultant

Lori Shepard, Senior Intelligence Consultant

Paige Inscoe, Senior Intelligence Consultant

Diana Striedieck, Senior Intelligence Consultant

Sarah Kinzer, Senior Intelligence Consultant

Shelley Hills, Senior Intelligence Consultant

L-3 Communications

Tom Knapp, Principal Systems Engineer

Lance Call, Senior Software Engineer

Brent Nielson, Systems Administrator

Robert Creter, Systems Administrator

Workshop Attendees

Lt Col Reb Butler, 57th Information Aggressor Squadron

Mr. Todd Denning, 505th Operations Squadron

Lt Col Andrew Hansen, 18th Aggressor Squadron

James Hird, 688th Information Operations Wing

Dr. Gary Klein, Klein Associates Division of ARA

Dr. Alex Levis, George Mason University

Lt Col Matteo Martemucci, 547th Intelligence Squadron

Dr. Greg Zacharias, Charles River Analytics

Other Contributors

Mr. Al Gonzalez, 23rd Information Operations Squadron

Maj Magoo Bakshas, 33rd Information Operations Squadron

Capt Mike Jansen, 346th Test Squadron

Mr. Scott Runyan, 39th Information Operations Squadron

Col Edward McKinzie, 505th Command and Control Wing

Lt Col Greg Brown, 547th Intelligence Squadron

Mr. Larry Shoger, 547th Intelligence Squadron

Lt Col Roger Trueblood, 547th Intelligence Squadron

Capt Brandon Stoker, 547th Intelligence Squadron

Mr. Lou Giannelli, 547th Intelligence Squadron

Lt Col Timothy “Chewy” Franz, 57th Information Aggressor Squadron

Capt Karson Kuhlman, 57th Information Aggressor Squadron

Capt Jeffery Jeffers, 67th Network Warfare Wing

TSgt Kirk Zinnell, 67th Network Warfare Wing

Maj John “Drayco” Henley, 318th Information Operations Squadron, Detachment 2

Dr. Janet Fender, Air Combat Command

Mr. Stan Newberry, Air Force Command and Control Integration Center

Mr. Bill Underwood, Air Force Information Operations Wing

Mr. Mike Kretzer, Air Force Information Operations Wing

Capt Brail, Air Force Information Operations Center /IOT

Capt Mackenzie, Air Force Information Operations Wing Commander’s Action Group

Capt Christian Fisher, 318th Information Operations Squadron, Detachment 2

Capt Jack “Tandy” Galloway, 318th Information Operations Squadron, Detachment 2

MSgt Daryl Crissman, Air Force Information Operations Center Detachment 2

TSgt Medrano, 318th Information Operations Squadron, Detachment 2

Mr. Thomas May, Air Force Network Integration Center

Dr. Kristen Liggett, Air Force Research Laboratory /RHCV

Dr. Joe Lyons, Air Force Research Laboratory /RHXS

Dr. John Salerno, Air Force Research Laboratory /RIEF

Dr. Elizabeth Kean, Air Force Research Laboratory/RISA

Lt Col Steve Katz, Air Force Space Command

Mr. Steve Brueckner, ATC-NY

Mr. Chris Lyons, Joint Forces Command Joint IO Range LNO to Nellis AFB

Mr. David Mauroni, National Air and Space Intelligence Center

Mr. Steve Wright, National Security Agency Liaison Officer to Nellis AFB

Dr. Eduardo Salas, University of Central Florida

9 Appendix B
Glossary of Acronyms

Acronyms

AAR After-Action Review

ABM Air Battle Management

ACC Air Combat Command

ADDIE Analysis Design Development Implementation Evaluation

AETC Air Education Training Command

AF Air Force

AFB Air Force Base

AFIOC/ IOT Air Force Information Operations Center Information Technologies Division

AFIT Air Force Institute of Technology

AFRL Air Force Research Laboratory

AFSC Air Force Specialty Code

AOC Air and Space Operations Center

API Application Programming Interfaces

ASKAS Air Superiority Knowledge Assessment System

C/S/A Combatant Commands, Services, Agencies

C2 Command and Control

C2WSPTT Command and Control Weapons System Part-Task Trainer

C2WT C2 Wind Tunnel

C4 Command, Control, Communications, Computers

C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CAI Computer-aided Instruction

CAT Coordinated Attack Tool

CBT Computer Based Training

CDC Career Development Course

CERT Computer Emergency Response Team

CFETP Career Force Education and Training Plans

CND Computer Network Defense

CNDSP Computer Network Defense Service Providers

COCOM Combatant Command

CONUS Contiguous United States

COVE Cyber Operations Virtual Environment

CPAS Combined Air Operations Center Performance Assessment System

DCIO Defense Criminal Investigative Organization

DIS Distributed Interactive Simulation

DMT Distributed Mission Training

DoD Department of Defense

DOS Denial of Service

EW Electronic Warfare

FLEX Flexible Method of Cognitive Task Analysis

FSVE Full-spectrum Virtual Environment

FTU Formal Training Unit

GIG Global Information Grid

HLA High Level Architecture

IA Information Assurance

IDS Intrusion Detection System

IOS Information Operations Squadron

IP Internet Protocol

ISD Instructional Systems Design

ISR Intelligence Surveillance and Reconnaissance

IT Information Technology

ITS Intelligent Tutoring System

JIOR Joint Information Operations Range

JTF-GNO Joint Task Force-Global Network Operations

JTF-GNO LECIC JTF-GNO Law Enforcement and Counterintelligence Center

LARIAT Lincoln Adaptable Real-Time Information Assurance Testbed

LCD Learner-Centered Design

MA Mission Assurance

MEC Mission Essential Competency

MUTT Multi User Training Tool

NAE National Academy of Engineering

NCW Network Centric Warfare

NETA Network Attack

NETD Network Defense

NOSC Network Operations and Security Center

NTOC National Security Agency/Central Security Service Threat Operations Center

NWW Network Warfare Wing

ORA Operational Requirements Analysis

PETS Performance Effectiveness Tracking System

S & T Science and Technology

SA Situation Awareness

SAB Scientific Advisory Board

SAST System Administrator Simulation Trainer

SCADA Supervisory Control and Data Acquisition

SIMTEX Simulator Training Exercise

SOP Standardized Operating Procedure

TADMUS Tactical Decision Making Under Stress

TRT Training and Rehearsal Testbed

TSA Team Situation Awareness

TTL Training Task List

TTP Tactics Techniques and Procedures

UNWT Undergraduate Network Warfare Training

USAF United States Air Force

USSTRATCOM United States Strategic Command

VE Virtual Environment

VLE Virtual Learning Environment

WS Weapon System

ZPD Zone of Proximal Development

10 Appendix C
Analysis of Cyber-relevant Learning Objectives and MEC Knowledge and Skills

To form our instructional S & T recommendations for the AOC (summarized in Section 5), we conducted an analysis of the existing learning objectives. This analysis aimed to identify cyber-relevant learning objectives as reflected in training curricula and official documentation.

Survey of AOC Learning Objectives and Curriculum

Efforts were initiated to develop an understanding of current curricula, learning objectives, and relevant research concerning mission assurance and cyber threats. These efforts included outreach to operational and training communities and the findings are based on conversations with Lt Col Dean Clothier, 39 IOS/CC, Mr. Scott Runyan, 39 IOS Undergraduate Network Warfare Training Course director/DoD Contractor, Lou Gianelli, 547th Intelligence Squadron (a former supervisor of an AF Network Operations Security Center (NOSC)), Mr. Jim Hird, Chief, AFIOC Modeling and Simulation (a former Commander of a Communications Squadron supporting the Nellis Range Operations) and both Ms. Lori Shepard and Ms. Diana Striedieck, PatchPlus Consulting Senior Intelligence experts (experienced in both AOC operations and training). The assessment included a review of USAF training plans and task lists, as well as a series of interviews. The interviews were conducted with professional communications officers, cyber defenders, and former students and employees of the 505 CCW AOC Formal Training Unit (FTU). These activities were specifically undertaken to ascertain the extent of formal training focused on cyber-relevant TTPs for the AOC.

AOC communications staff training

We concluded that current AOC communications staff structures do not explicitly specify inclusion of trained network defenders on staff. Further, staff assigned as AOC help desk operators are trained in AOC-specific software and applications in the event of a technical problem or training deficit by an operator. Thus, they do not primarily serve as network defenders but as computer systems administrators in the AOC. However, according to the minutes of a 9-11 February 2010 AOC FTU Syllabus Review Conference, the decision for more robust training on current threat possibilities facing AOC networks has been made and will be developed in the near future (Hazeur, 2010). This does not include assigning computer network defenders to the AOC but it does address teaching the AOC staff how to work through network threats and increase threat awareness in general. For now, the NOSC staff serves as the network “watchdog” for the entire Unites States Air Force (USAF). Their services include analysis of logs, security events, active vulnerability scanning, bandwidth management, address and space management and other functions.

In the AOC, until December 2009, the standard communications personnel manning included Communications-Computer Systems Operators (AFSC 3C0X1), Electro-Magnetic Spectrum Managers (AFSC 3C1X2), and Network Integrators (AFSC 3C2X1). A review of the CFETPs for these AFSCs indicated these personnel receive some basic IA-type knowledge at their initial skills training course and in their Career Development Course (CDC) about general system vulnerabilities and the concepts of identifying and reporting intrusion incidents. However, at no point did they receive any task performance training on identifying and reporting such incidents. More importantly they receive no training on the mission assurance functions of planning or executing MA tasks for fighting through cyber attacks.

The AF is currently transitioning both officers and enlisted from communications AFSCs to the new cyber career fields. The AF has automatically converted all Communications Officers (AFSC 33S) to the new Cyber Operations AFSC 17D. A computer-based conversion course has begun (as of late 2009) to offer some cyber knowledge but the robust, 23-week, in-residence course will not be up and running until mid- to late 2010 (http://www.keesler.af.mil/news/story.asp?id=123164133). The new course curriculum includes seven key areas: technical fundamentals, expeditionary communications,

information assurance, net defense, attack and exploit, information operations and a capstone exercise entitled "Fighting Through an Attack." Based on our understanding of this exercise, we conclude that this capstone exercise would provide quality training for the System/Network Administrators and Cyber Warriors but not End User (Warriors). General Lord (SAF/XC) is overseeing the project and Lt Col Joe Trechter SAF/XCTF and Maj Joe Stockton at Air Education Training Command (AETC)are leading the curriculum development. The formal training for both officers and enlisted will take place at Keesler Air Force Base, MS (http://www.keesler.af.mil/news/story.asp?id=123157023) with a Network Operations FTU follow-on at Hurlburt Field, FL.

In the future, there will likely be cyber operators (specifically computer network defenders) on staff in the AOC but this possibility is likely a number of years from fielding. The enlisted force has already transitioned from the former 3AXXX and 3CXXX to the new 3DXXX (cyber) AFSCs and although IA and network operations training is much more robust, the practice of mission assurance is not incorporated into the training at the basic levels.

At the AOC FTU at Hurlburt Field, FL, training of communications personnel is sorted by position, including: (1) Chief, (2) Work Group Management (WGM)/Section Supervisor, (3) Information Management (IM) – Web/Datawall, (4) Job Control, and (5) Help Desk. A review of the Communications AOC Master Training Task List revealed that no position receives task performance training on cyber-relevant TTPs during IQT. The chief and WGM/Section Supervisors are briefed on basic knowledge about identifying communication vulnerabilities, deliberate communication attacks and alternate procedures. This should increase trainees' knowledge of factual information about these topics, but they receive no skill training for performing MA functions. Conversely, the IM-Web/Datawall, Job Control, and Help Desk personnel are supposed to receive informal task training on cyber defense functions during Mission Qualification Training once they return to their assigned unit. Discussions with communications personnel indicate the MQT task training at the units may be more IA focused rather than MA-focused.

Our review of the AOC FTU Training Task Lists (TTLs) for non-communications personnel, our previous experience with the AOC FTU, and our interviews with students from the AOC FTU indicate a lack of MA training for non-communications personnel. The AOC FTU indicates that a lack of AOC Weapon System (AOC WS) standardized operating procedures (SOPs) prevents them from being able to train students how to accomplish their responsibilities. There are no process-oriented checklists dictating how data should be stored or retrieved. Rather students are taught basic uses of AOC WS applications and then must determine for themselves, during the End of Course Exercise, what applications to use for whatever processes they must accomplish as well as the actual procedures for entering, storing, and retrieving data. The current AOC FTU system training creates at least two problems from a MA training perspective. First, because the trainees do not understand where or how their data is stored and exchanged with other applications/systems, both internal to and external from the AOC, they have no concept of their data vulnerabilities, much less how to identify any potential corruption/malicious activity. Second, due to the lack of standardized weapon system procedures, the students are unable to differentiate between mistakes they've made in entering or retrieving data, system/network problems or errors and indications of malicious enemy activity. Moreover, the lack of any formal knowledge training in their AOC FTU courses about MA and the AOC WS vulnerabilities leaves the students without awareness of such vulnerabilities and without a notion of how to counter or fight through a cyber attack and ensure continued mission accomplishment.

The 705th Combat Training Squadron (705CTS) develops and conducts advanced AOC training courses for senior AOC crew positions. A review of the draft TTLs for the advanced courses, circa 2007, revealed not only a lack of cyber-relevant TTP training but also a lack of systems-specific training. Subsequent

discussions with former employees and students indicate these courses continue to lack any cyber-relevant TTP training focus.

Overall, we concluded there is currently little or no formal cyber-relevant TTP training accomplished in the AFSC technical schools at AOC schools at Hurlburt Field. Further analysis, as described in the following sections, focused on MECs and joint doctrine and were used as a supplement to the analysis of training curricula and learning objectives.

AOC MECs

We conducted a review of MEC summary documents for the Strategy, Plans, Operations, and Intelligence Surveillance and Reconnaissance (ISR) divisions of the AOC. Our focus was primarily on the identification of potential training gaps relative to cyber-relevant TTPs. We reviewed each individual element (a high-order competency, an experience, or a knowledge/skill) and judged whether that element was related to a capability that possibly increased sensitivity and responsiveness to cyber attacks – by either facilitating detection of cyber attacks or capabilities to fight through attacks. Virtually no high-order competencies meet this criterion. Across the four domains, very few experiences were judged to be relevant to cyber attack (an overall average of 5%). Similarly, very few knowledge and skills were judged as relevant to cyber attack (an overall average of 5%). The authors judge it important to note that <u>no</u> high-order competency, experience, or knowledge/skill for any division of an AOC explicitly identifies or refers to cyber attacks. Thus, the 5% of relevant experiences, knowledge, and skills we report to be relevant to cyber warfare should be viewed as an optimistic estimate of the attention being paid to cyber relevant issues at the time these MEC materials were created.

Joint doctrine

We also conducted a review of joint doctrine prescribing the required coordination between network/system administrators and cyber warriors (Joint Chiefs of Staff, 2009). One characterization of the role, responsibilities, and dependencies of these user groups is depicted in Figure 44. This figure illustrates the interdependencies between players in terms of incident reporting and the distribution of guidance. This figure does not illustrate the required coordination between end users and other groups. Team-of-teams training opportunities should account for the dependencies between end users and the groups referred to in Figure 44. We recommend that future systems not only enable instructionally sound training opportunities, but also provide opportunities for interaction across the interdependent parties.

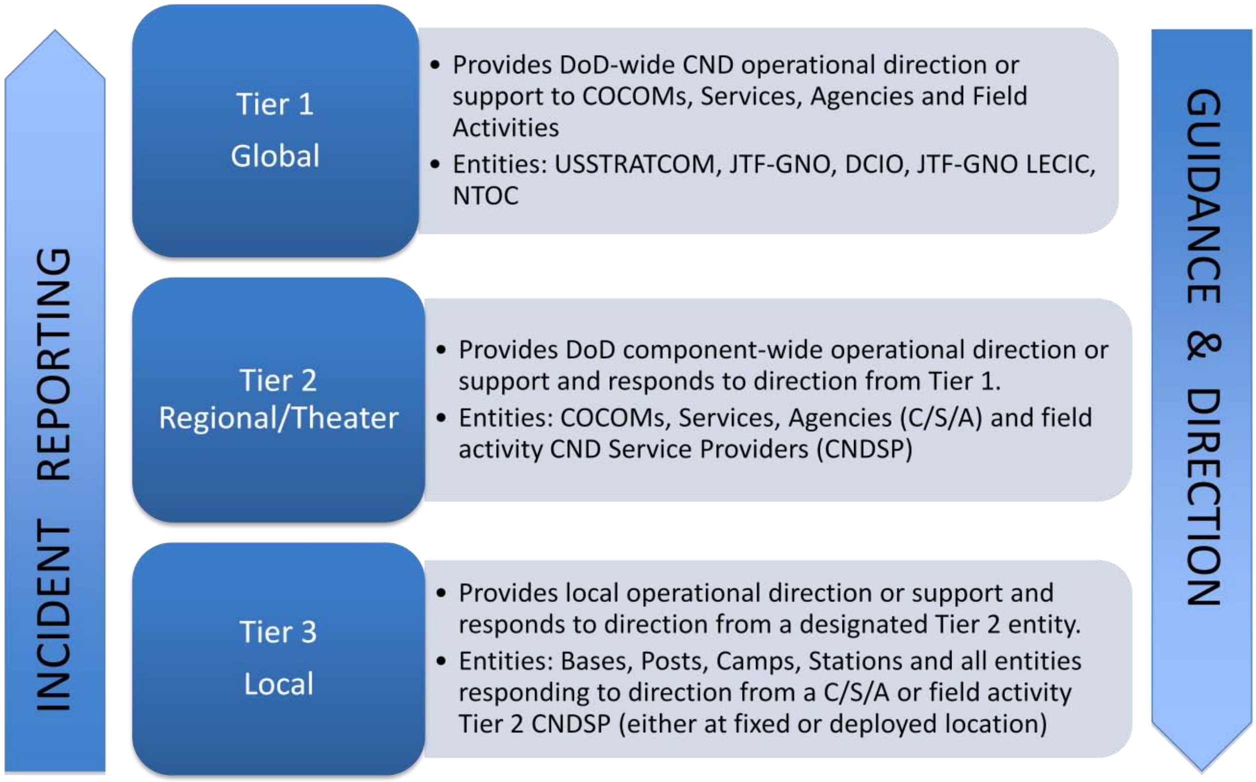

Figure 4. Joint incident reporting process

Identified gaps

A review of training curricula, MECs, and joint doctrine revealed that, until recently, cyber-specific training has not been an area of focus. Accordingly, there is a significant lack of learning objectives addressing the cyber domain and fighting through attacks to achieve mission assurance. Operational TTPs and learning objectives are likely to develop in parallel as focus on cyber threats increases. As this occurs it will be important to maintain focus on the various user groups who are reliant on each other to achieve mission assurance. Information, responsibilities, and capabilities are distributed across groups and not all users are equipped with IDS systems to detect current cyber attacks. Mission assurance will require a united response, leveraging the expertise and capabilities of network/system administrators, cyber warriors, and end users. It is critical that any defined learning objectives account for the dependencies that exist between these user groups.

12 Appendix D
Survey of Cyber Simulation and Training Technology

Survey of Cyber Simulation and Training Technologies

According to the SAB, the single most important shortfall observed with respect to cyber attacks is that the USAF is not prepared to fight through (2007a). The SAB members attribute this lack of preparedness to what they observe is a lack of integration of cyber warfare training within conventional operational training (2007b). The lack of integration of cyber attack elements within conventional training limits the Airmen's ability to experience the attacks, understand the effects, and "learn how to work through and defeat a combined attack, even with compromised systems" (2007b, p. 38).

The cyber domain has seen an increase in the development of simulation and training capabilities (e.g., Brueckner, Guaspari, Adelstein, & Weeks, 2008; Wabiszewski, Andel, Mullins, & Thomas, 2009; see also Katz, 2010). These systems provide new capabilities including traffic generation and cyber threat simulation. End Users (Warriors), System/Network Administrators, and Cyber Warriors will rely on such systems to prepare for cyber threats. However, the existing cyber simulation and training systems we reviewed do not represent the type of comprehensive instructional environments as we are recommending in this S & T plan. We attribute this to the fact that cyber-related learning objectives are simultaneously emerging as these systems are being developed. Practice in the absence of instructional support is less than optimal, and it is essential for training scenarios and exercises to be tightly linked to learning objectives. Nonetheless, the system development occurring is laying a foundation for comprehensive instructional environments.

Cyber tools and systems may be characterized in a number of ways. For instance, they may be thought of as belonging to one of three distinct categories: individualized training systems, full-spectrum virtual environments (FSVE), and building blocks. Individual training tools are primarily used for training of individual operators and may restrict their focus to either a limited number of competencies or to generalized training of cyber skills, whereas full-spectrum virtual environments tend to train large numbers of individuals at any one time, are more focused on USAF training exercises, and can support the training of a wide range of cyber competencies per individual. Building blocks are essentially components that can be built upon or integrated with other systems, but otherwise have limited utility as stand-alone systems.

Individualized training systems

In a comprehensive learning environment to support cyber skill development, individualized training systems play a role in achieving instructional objectives which are highly focused and/or are intended to train individuals in specific areas (e.g., detection). An individualized training system may consist of a combination of a virtual network, one or more cyber attack simulations, and either real or virtualized operator stations, connected together via a local Ethernet to provide a training/rehearsal environment in which an individual may exercise routine skills in network administration and cyber defense. Individualized training systems may be limited in the number and type of networks that can be represented as well as the type of training and number of users. Due to their smaller footprint and system administration overhead when compared to a full-spectrum virtual environment, individualized training systems may be more suited for wide distribution across a number of AF training sites and may present increased opportunities for continuing training.

Full-spectrum virtual environments

In contrast to individualized training systems are FSVEs which provide a complete training landscape, replicating real-world (actual) networking/cyber defense/cyber attack to a high degree of fidelity, and

including instructional support functionality (e.g., automated performance measurement or replay functionality to support AAR). A key feature of an FSVE is that it incorporates real-world physical networking hardware, which allows for accurate representation of real-world cyber attacks. These environments provide a “sandbox” which allows operators to train as if in an operational environment; the sandbox is isolated from any operational equipment or networks and thus can “sustain” cyber damages, with no negative effects felt outside the sandbox. Within the virtual sandbox, operators are able to experience and train against actual cyber attacks. When training objectives for a particular scenario have been met, the virtual environment can be reset to a clean state and is ready to deliver another training scenario. Training systems of this nature support the requirement of realistic and relevant context from social constructivist learning theory.

It should be noted that large-scale exercises conducted in FSVEs are inherently limited due to the expense of implementation and the resulting lack of diversity and replication of scenarios. In addition, in most large-scale exercises performance measurement does not occur at a level of specificity to provide meaningful feedback to enhance the learning experience for all participants involved.

SIMTEX, a testing and training environment for network tacticians, is the closest example of an FSVE that we were able to identify but it has its limitations. SIMTEX has supported the joint exercise Bulwark Defender since its inception in 2006. Since the early days of exercise Black Demon in 2002 and 2003, SIMTEX has provided a safe environment for the 23rd Information Operations Squadron (23 IOS) to develop and test the network tactics and train network tacticians through the Network Tacticians Course (NTC). At the Air Force’s Undergraduate Network Warfare Training Course (UNWT) at the 39 IOS on Hurlburt Field, FL, SIMTEX simulators provide testable content. Students apply the theory they learn in a hands on environment to stop real attacks against their classroom simulators (T. May (AFNIC), personal communication, March 17, 2010). Limitations such as a lack of performance measurement and scenario replay capabilities prevent SIMTEX from being a true FSVE.

Building blocks

A third category identified in this effort is that of building blocks which can serve as a framework upon which additional cyber training capabilities may be developed. Capabilities within this category may not directly provide cyber training as an out-of-box feature; rather, this category focuses on the tools and systems that model to varying degrees the environment or the network protocol itself. The functionality of these building block capabilities varies, and ranges from providing an infrastructure that models an environment or subset of an environment (such as the USAF AOC environment) to providing a set of Application Programming Interfaces (APIs) upon which cyber training tools may be built. An example of the former includes the C2 Wind Tunnel (C2WT), and an example of the latter includes the open-source OMNeT++ framework. The C2WT may be characterized as a collection of analytical models. In comparison, tools such as OMNeT++ provide the building blocks upon which networks may be designed and provide features such as network traffic modeling (e.g., Transmission Control Protocol [TCP]/Internet Protocol [IP]) and discrete event modeling within a network.

Other examples of building blocks and the capabilities they could provide for a comprehensive virtual learning environment include:

- QualNet: A network simulation tool that simulates wireless and wired networks [http://www.scalable-networks.com/products/qualnet/]. QualNet could provide network simulation models for a wide variety of networks, including Link16, Link11, satellite networks and wireless networks.

- IT Sentinel: a "software appliance for ensuring network integrity, security, and policy-compliance". (http://www.opnet.com/solutions/network_planning_operations/it_sentinel.html). IT Sentinel could provide network monitoring and policy compliance capabilities.
- Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT): LARIAT was designed to support real-time evaluations and serve as a deployable, configurable testbed. LARIAT could provide information assurance capabilities as well as provide scripted attacker and background traffic. LARIAT may be used to generate cyber attacks for known exploits (see Rossey et al., 2001).
- JFCOM Joint Information Operations Range: The JIOR isolates cyberspace effects from the public Internet while protecting tactics, techniques, and procedures from observation by potential adversaries (see http://www.jfcom.mil/about/fact_iorange.html). An interface to the JIOR could provide additional training opportunities for cyber warriors.
- System Administrator Simulation Trainer (SAST): SAST provides multi-user training opportunities for students to defend against cyber attacks via the SAST Coordinated Attack Tool (CAT); CAT simulates real-world cyber attacks and is based on existing hacker tools and scripts (see Okolica, McDonald, Peterson, Mills, & Haas, 2009). SAST also allows users to train against traffic from large numbers of typical networks users (email, web browsing, etc.) through traffic generated from its Multi User Training Tool (MUTT).

Building blocks will generally be used as "starting points" from which cyber training capability will be developed. Building blocks often combine with other tools in this or other categories to achieve a desired cyber training capability; capabilities in this category typically contain features which may be useful to a larger cyber training capability but whose individual capabilities are not sufficient to provide cyber training. Building blocks are envisioned as potential enhancements to individual training systems or full spectrum virtual environments. As such, the tools and systems in the building blocks category are typically not used directly as training aids for Airmen.

Instructional capability gaps

No existing cyber technologies could be truly classified as a FSVE, as they did not include both the essential components of the environment <u>and</u> the instructional capabilities to support learning. We recommend the following set of requirements be used to evaluate and guide the design of cyber systems:

- Well-specified learning objectives to support competency-based training
- Realistic context which presents cyber threats and effects from other arenas including kinetic and electronic warfare
- Scenario development to incorporate cyber threats as triggers to elicit behaviors
- Context-rich situations and scenarios to enable practice of learning objectives and performance measurement and error diagnosis
- Scenario reset and rerun capability
- Reproducible scenarios
- Appropriate levels of task fidelity
- Performance measurement capability to inform feedback
- Opportunities for practice within a team context